Noname manuscript No.
(will be inserted by the editor)

Adaptive Wireless Communications under Competition and Jamming in Energy Constrained Networks

Zaheer Khan, Janne Lehtomäki, Athanasios V. Vasilakos, Allen B. MacKenzie, and Markku Juntti

the date of receipt and acceptance should be inserted later

Abstract We propose a framed slotted Aloha-based adaptive method for robust communication between autonomous wireless nodes competing to access a channel under unknown network conditions such as adversarial disruptions. With energy as a scarce resource, we show that in order to disrupt communications, our method forces the reactive adversary to incur higher energy cost relative to a legitimate node. Consequently, the adversary depletes its energy resources and stops attacking the network. Using the proposed method, a transmitter node changes the number of selected time slots and the access probability in each selected time slot based on the number of unsuccessful transmissions of a data packet. On the receiver side, a receiver node changes the probability of listening in a time slot based on the number of unsuccessful communication attempts of a packet. We compare the proposed method with two other framed slotted Aloha-based methods in terms of average energy consumption and average time required to communicate a packet. For performance evaluation, we consider scenarios in which: 1) Multiple nodes compete to access a channel. 2) Nodes compete in the presence of adversarial attacks. 3) Nodes compete in the presence of channel errors and capture effect.

Index Terms:
Autonomous nodes, distributed networks, robust protocol, adaptations, reactive adversary, jamming, energy-constraints.

I Introduction

The need to design access schemes for various new applications in machine-to-machine (M2M) communications , wireless social networks, and sensor networks has led to re-

Centre for Wireless Communications
University of Oulu, Oulu
Erkki Koiso-Kanttilan katu 3 90570 Oulu, Finland
Email: zaheer@ee.oulu.fi
Email: jannel@ee.oulu.fi

newed interest in research on random access protocols that enable secure co-existence among multiple wireless nodes [1–3]. In such applications, wireless nodes are often battery powered, autonomous, and operate in uncertain and dynamic environments. Without proper measures, the autonomous nature of nodes operating in such systems makes them vulnerable to *adversarial disruptions*. The sources of adversarial disruptions can be diverse. For example, disruptions could be due to nearby nodes following unrelated protocols, a faulty device, or an actual adversary intentionally disrupting communication in the network. Moreover, due to the dynamic and uncertain nature of wireless environment, the type of interference incurred by a node can change dynamically. For example, at a given time instant multiple nodes may be competing to access a shared medium, however, at a later time an adversary may become active in the network and attempt to disrupt the communications. In this example, initially the nodes need to co-exist with one another while minimizing interference, but later they also need to ensure successful communication in the presence of adversarial disruptions. One way to ensure successful communication is to allow the nodes to utilize adaptive randomized communication access methods.

In this paper, we consider scenarios where multiple nodes with energy and information constraints are competing for access over a shared medium and may face reactive adversarial disruptions. Energy constraints mean that the nodes are battery powered and information constraints imply that the nodes do not have any information about the type of other nodes and also they do not share any information among one another.

In the scenarios where the nodes operate autonomously it is likely that all nodes, including adversarial nodes, have energy constraints. In such scenarios, it seems reasonable to consider a notion of relative cost in terms of energy. The following example illustrates this notion of relative cost in terms of energy. Consider an autonomous TX node that wants to communicate M packets to its intended RX node in the presence of a reactive adversary node that wants to disrupt them. Suppose that each node is battery powered with a total energy budget of B units. Consider the case where the energy spent in a transmission attempt of a packet by the TX is C_T units, and the energy spent in a reception attempt of the packet by the RX is C_R units. If the adversary can successfully jam the packet by spending C_J units of energy, where $C_J < C_T$ or $C_J < C_R$, then the adversary can completely jam the communications between the TX and the RX, as either the TX or the RX will completely deplete their energy before the adversary. Using this notion of relative cost, we ask the following question in this work: Does our designed protocol ensure that it is significantly more costly for a reactive adversary to disrupt communications than for a TX and an RX node to communicate? Our answer is yes. In other words, our protocol forces the adversary to incur higher energy cost relative to a legitimate node and guarantees successful communication of packets.

Our main contributions in this paper are:

1) We propose and evaluate an *adaptive robust* method called Adapt-R. Using analytical and simulation results, we show that our proposed method reduces the likelihood of collisions among competing legitimate nodes. Hence, it reduces the communication attempt costs in terms of energy and delay;

2) We then explore the robustness of the proposed method against adversarial disruptions. We present analytical and simulation results in terms of average energy cost incurred by a legitimate node to communicate data packets successfully in the presence of adversary;

3) We also compare the energy and delay costs incurred using the proposed method with the energy and delay costs with three other methods;

4) Finally, we explore the impact of channel errors and capture effect on the performance of the proposed method. We also explore the impact of varying energy costs incurred by the nodes on the performance of the proposed method.

II Related Work

Different variants of slotted Aloha and framed slotted Aloha protocols have been proposed in literature for various applications [1, 2, 4–6]. For instance, the framed slotted Aloha-based access schemes are used in a number of RFID communication protocols and has also been studied for applications in sensor networks and M2M communications [1, 2]. The works in [4–6] consider the scenarios where multiple transmitters (TXs) communicate with a single receiver. Unlike the works in [4–6], we consider a single channel wireless network of N distributed TX/RX pairs.

There has been considerable research in studying the problem of competition [7, 8] and conflict (adversarial disruptions) in a shared medium access [9–11]. Moreover, recent works in [10, 12] have practically demonstrated that flexible and reliable software-defined reactive jamming is feasible by designing and implementing a reactive jammer against existing wireless networks. However, most existing research either does not take into account the energy expenditures of the adversary and the legitimate nodes or it consider the energy expenditures of the legitimate nodes and the adversary in isolation (see [13–16] and [17], and references therein). In autonomous scenarios where energy is a scarce resource for both the legitimate competing nodes and the adversary it is reasonable to consider a notion of relative cost in terms of energy. The authors in [18] follow this idea to design a protocol for the scenario where a transmitter has a single packet to communicate to a particular receiver in the presence of a reactive adversary. The authors show that it is possible to design a protocol which ensures that it is cheaper in terms of energy for a transmitter to successfully transmit a packet to its intended receiver than for an adversary to block this packet. Different from [18], in this paper, we consider scenarios where multiple TX/RX pairs communicate in the presence of competition and reactive jamming, and each TX has more than one data packet to communicate to its intended RX. A game-theoretic model of the interactions between nodes exploiting the timing channel to achieve resilience to jamming attacks and a jammer is studied in [19].

In [20], a novel agent-based Trust and Reputation Management scheme (ATRM) is presented from a system design point of view. The authors presented a trust and management strategy and showed that the proposed strategy reduces both communication cost and acquisition latency. The security properties of a multicast scheme for sensor based healthcare systems are studied in [21]. This work also discusses the innovation and design requirements of novel trust based models that use ad hoc sensor networks to collect data from the patients. Security and privacy issues relating to wireless communications based health care systems is the topic of [22]. Several diverse factors that take part in the design of reliable, intelligent, secure patient monitoring and management systems has been presented in [22]. A novel and efficient energy-aware distributed method for data delivery in wireless micro sensor networks is presented in [23]. The method proposed in [23] makes no assumption on local network topology, and is based on residual energy of the sensor nodes. The works in [24] focuses on several fundamental algorithms and protocols for the next generation of wireless networks. In [25], a detailed survey relating to the Internet of Vehicle is presented. The work in [25] also explains the requirements for efficient security support relating to the next generation of networks. Quality of service, energy efficiency and security issues relating to machine-to-machine (M2M) networks are presented in [26]. The work in [27] presents quality of service and quality of data oriented architecture for the industrial wireless networks.

Most research on reliable communication between autonomous nodes competing in a shared medium has focused on the design of either *adversary-naive* or *adversary-paranoid* protocols. Adversary-naive protocols are designed under the assumption that all nodes competing to access a shared medium follow the protocol and ignore the possible presence of adversarial disruptions of communication in the network [28–30]. As a result such protocols are vulnerable to adversarial disruptions. On the other hand, adversary-paranoid protocols are designed under the pessimistic assumption that adversarial disruption sources are always present in the wireless network [18, 31]. However adversarial disruptions may not always happen, such scenarios are studied in [32]. The work in [32] assumes that nodes are equipped with intrusion detection systems and it designs defense strategies to detect malicious misbehavior in ad hoc networks where the defender is uncertain about the type of his opponent (legitimate or adversary). Different from [32] we do not assume that nodes are equipped with intrusion detection systems. Note that in practice, when an autonomous node communicates in the presence of legitimate competing nodes and an intelligent adversary then it may not be easily possible to detect whether the disruption is due to collision among legitimate nodes or due to intentional disruption of the adversary. In [33] the authors analyze the energy costs of jamming acknowledgement (ACK) attacks in IEEE 802.11 based MAC. A recent work in [34] designs energy efficient strategies from the jammer's perspective for the scenarios where the jammer disrupts communications to reduce the network throughput. Unlike [34], our work designs a protocol for efficient communication of multiple data packets and considers energy costs incurred by both legitimate and adversarial nodes.

III System Model

A Network Model

We consider a single-channel, distributed wireless network of N autonomous TX/RX pairs in which each TX/RX pair has M packets to communicate. The set of N TX/RX pairs is given by $\mathcal{N} = \{1, 2, \ldots, N\}$. Each TX/RX pair operates using a framed slot-

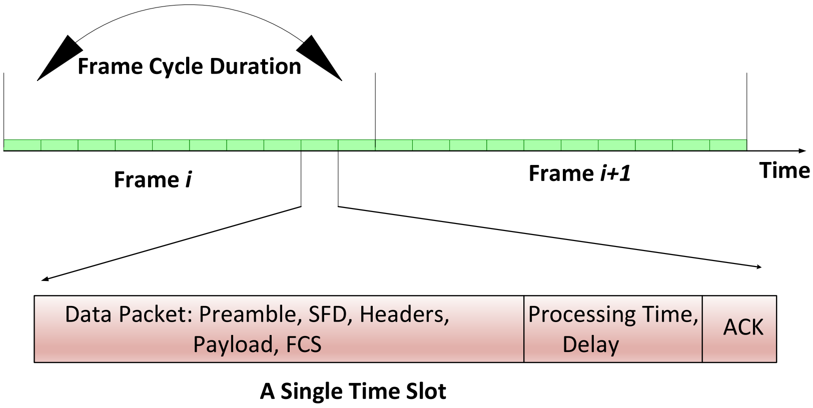


Fig. 1: Framed slotted Aloha-based time slot structure.

ted Aloha-based communication scheme. Although this scheme is fundamentally a contention-based random access scheme, we allow a TX/RX pair to "capture" a slot across multiple frames to improve MAC efficiency in a TDMA-like manner. Time is divided into slots and the number of time slots in a frame is denoted by s, where $s \geq 3$. We use a slot size such that a data packet and its associated ACK fit in a slot. After the transmission of a data packet, a TX node waits for ACK reception for a fixed time and, if no ACK is received during the specified time, then it infers that a collision has occurred. This transmission model is also adopted in several other works (see [35,36], and references there in). A frame structure of our framed slotted Aloha-based communication model is illustrated in Fig. 1. After successfully communicating M packets, the communication between a TX and its intended RX is terminated. In our model, there is no information exchange among the TX/RX pairs to access the channel, and the communication of packets is performed by each autonomous TX/RX pair based on the proposed distributed communication protocol, as explained in the subsequent section. Moreover, we consider battery powered TX/RX pairs with a limited energy budget of B units, where B is sufficiently large.

Note that in practice to conserve energy of distributed TX/RX pairs, each TX/RX pair should be put to *sleep mode* as soon as there is no more data to send/receive, and should be put to *awake mode* as soon as new packets become ready. Several distributed sleep/wakeup scheduling algorithms to conserve energy are presented in the literature (see [17,37] and references therein) and the study of such algorithms is beyond the scope of this paper.

B Adversary model and imperfect channel

In our model, the adversary is: 1) oblivious: knows the protocols of the TX/RX pairs, but does not know the randomized results of the protocol, such as which time slots are selected for transmissions and what is the access probability in the selected time slots; and 2) reactive: able to launch an attack after listening to a time slot. To disrupt communication, the adversary can utilize one of the following attack strategies: 1) Sequential jamming strategy (J_s). 2) Arbitrary jamming strategy (J_a).

Sequential jamming strategy: In each frame, a jammer listens sequentially in each time slot until a transmission from a TX is detected, if any, then jam the remaining portion of that time slot and wait for the next frame.

Arbitrary jamming strategy: In a frame, select s_J time slots (randomly with uniform distribution), where s_J can be any number from 1 to s, listen in each selected time slot and jam the remaining portion of the time slot/slots in which the transmission is detected.

The adversarial node can join the network of N competing TX/RX pairs any time. Similar to each of the legitimate TXs and RXs, the adversarial node also has the same energy budget of B units. We consider the worst-case scenario that when the reactive adversary joins the network it is synchronized with legitimate TX/RX pairs. Under this assumption, a reactive adversary can listen in a time slot and effectively jam the communication. If the jammer is not synchronized, then it may have difficulties in detection/jamming the communication effectively. For instance, it may happen that a jammer detects communication in time slot t but it jams the time slot $u = t + 1$ as due to non-synchronized operation it is operating over two different time slots. This will lead to energy waste for the adversary and hence can be beneficial for the legitimate TX/RX pairs.

Note that a TX on its own cannot differentiate whether the failure to receive an ACK is caused by a collision with the other competing TX, or due to a channel error or by adversarial jamming. In practice, failure to receive an ACK can be due to a channel error introduced by fading. Moreover, in practice interference can also be tolerated due to capture effect. In particular, due to co-channel interference tolerance, a transmission may still be correctly decoded by an RX even in the presence of interference in the channel. In Section V-F, we evaluate the impact of channel errors and capture effect on the performance of the proposed method.

C Energy cost model

We consider battery powered TX/RX pairs, and there is a cost of communication in terms of energy incurred to each TX and RX. We consider that the energy cost of a transmission in a time slot is S units, the cost of a listening in a time slot is L units and the cost of a jamming is J units. Note that the cost of sending and receiving data can be different. Moreover, transmitting/receiving an ACK does has not have the same cost as transmitting/receiving a data packet. To take this into account, in Section V-D, we evaluate the performance of the proposed protocol for different values of S, J and L.

In the next section, we present our proposed adaptive robust method named Adapt-R.

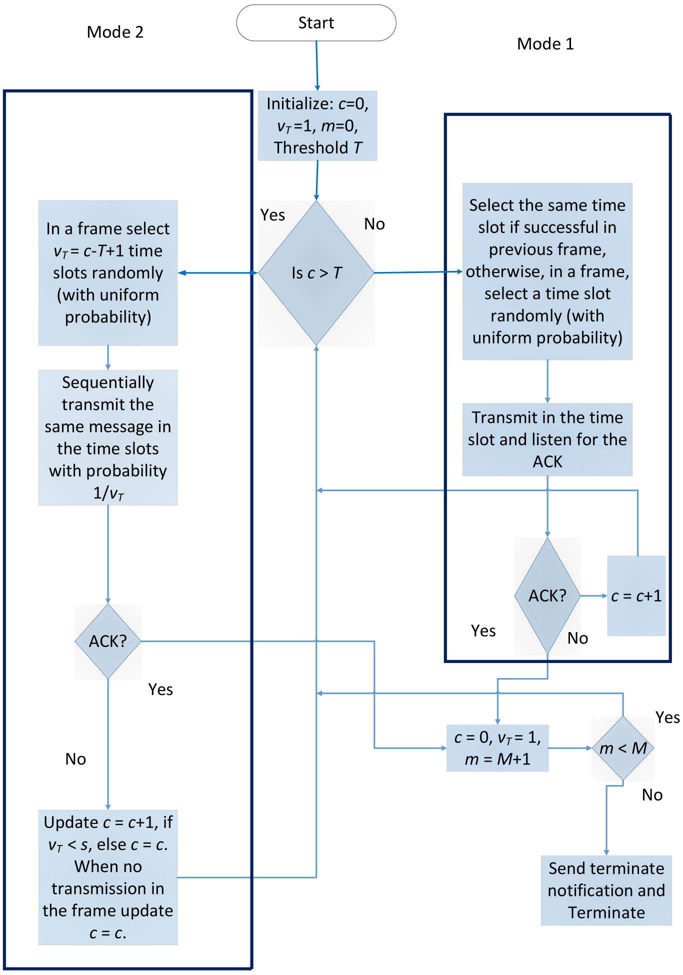

Mode 2
Start
Mode 1
Initialize: c=0, v_T=1, m=0, Threshold T
Yes
No
Is $c > T$
In a frame select v_T = c-T+1 time slots randomly (with uniform probability)
Select the same time slot if successful in previous frame, otherwise, in a frame, select a time slot randomly (with uniform probability)
Sequentially transmit the same message in the time slots with probability 1/v_T
Transmit in the time slot and listen for the ACK
ACK?
c = c+1
Yes
No
ACK?
Yes
No
c = 0, v_T = 1, m = M+1
m < M
Yes
No
Update c = c+1, if v_T < s, else c = c. When no transmission in the frame update c = c.
Send terminate notification and Terminate

Fig. 2: The Adapt-R method for a TX side.

IV Adaptive Robust (Adapt-R) method

The core idea of the proposed method is as follows:

- Using the proposed method, a TX changes the number of selected time slots and the access probability in each selected time slot based on the number of unsuccessful transmissions of a data packet.
- On the receiver side, an RX changes the probability of listening in a time slot based on the number of unsuccessful communication attempts of a data packet.

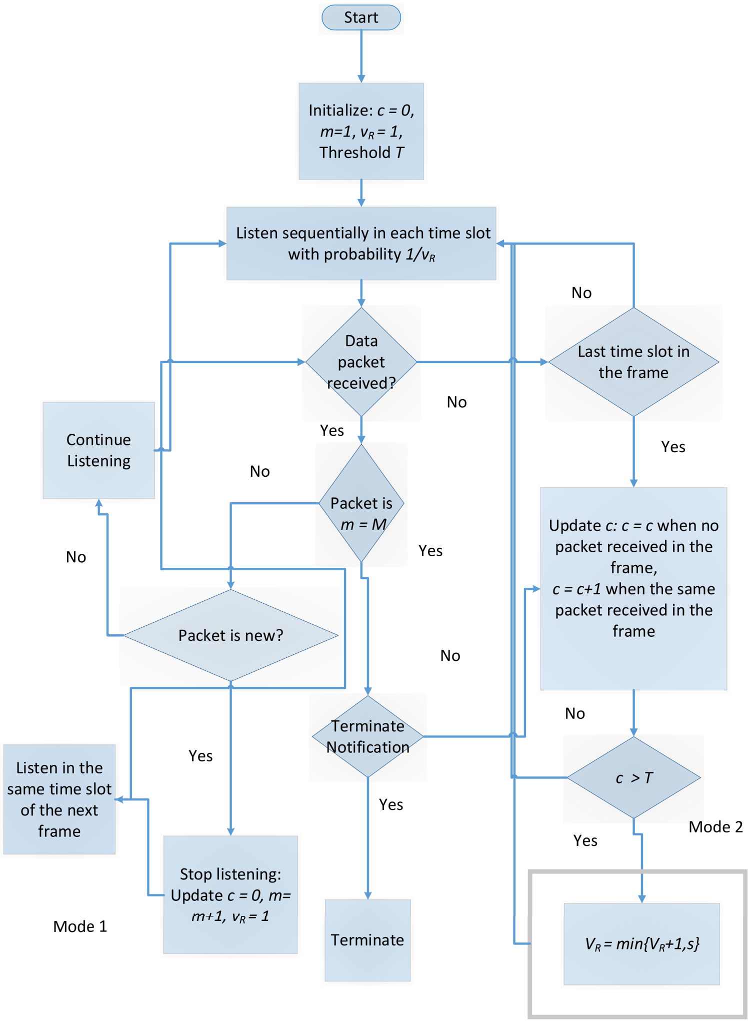

Start
Initialize: $c = 0$, $m=1$, $v_R = 1$, Threshold T
Listen sequentially in each time slot with probability $1/v_R$
Data packet received?
No
Yes
Last time slot in the frame
No
Yes
Packet is $m = M$
No
Yes
Continue Listening
No
Packet is new?
Yes
Update c: $c = c$ when no packet received in the frame, $c = c+1$ when the same packet received in the frame
No
Terminate Notification
No
Yes
$c > T$
Yes
Mode 2
Listen in the same time slot of the next frame
Stop listening: Update $c = 0$, $m=m+1$, $v_R = 1$
Terminate
$V_R = min\{V_R+1,s\}$
Mode 1

Fig. 3: The Adapt-R method for an RX side.

A Steps involved in the Adapt-R method

The developed method has two modes of operation: mode 1 and mode 2. Both TX and RX have their own counter c. The counter c is used to track the number of failures in communicating a particular packet and is also used to decide whether to operate in mode 1 or mode 2. The flow diagrams of the Adapt-R method are shown in Figs. 2

and 3, respectively. The two modes of the Adapt-R method are explained in detail as follows:

- *Mode 1 (TX side):* Initially, and also when the counter c is less than or equal to a threshold value T, a legitimate TX operates in mode 1. In mode 1, a TX randomly with uniform probability selects a time slot in a frame to transmit a packet and then listens for an ACK in that time slot. If the ACK is received, it sets $c = 0$, $\nu_T = 1$, and transmits the next data packet in the same time slot of the subsequent frame with probability one. Otherwise, it sets $c = c+1$ and selects randomly with uniform probability a time slot again.
- *Mode 2 (TX side):* When $c > T$, a TX operates in mode 2. In mode 2, a TX randomly with uniform probability selects $\nu_T = c-T+1$ time slots in a frame. It sequentially transmits the same packet in the selected time slots with probability $1/\nu_T$ and listens for an ACK in each slot. If it transmits and ACK is received it stops transmitting, it sets $c = 0$, $\nu_T = 1$, and transmits the new packet in the same time slot of the subsequent frame with probability one. If it transmits and no ACK is received, it sets $c = c+1$, if $\nu_T < s$, and else $c = c$. If it does not transmit in any time slot of the frame, it sets $c = c$.
- *Mode 1 (RX side):* Initially, and also when the counter c is less than or equal to a threshold value T, an RX operates in mode 1. In mode 1, an RX listens in each time slot of a frame sequentially with probability one. If it receives a new data packet from its intended TX, it stops listening and it sets $c = 0$, $\nu_R = 1$, and listens in the same time slot of the subsequent frame. Otherwise, it continues listening and if it receives the same data packet again, it sets $c = c+1$ at the end of the frame.
- *Mode 2 (RX side):* When $c > T$, an RX operates in mode 2. In mode 2, an RX listens in each time slot of a frame sequentially with probability $1/\nu_R$, where $\nu_R = \min\{\nu_R+1, s\}$. If it receives a new packet from its intended TX, it sets $c = 0$, $\nu_R = 1$, and listens in the same time slot of the subsequent frame. Otherwise, it listens in each time slot of a frame sequentially with probability $1/\nu_R$. At the end of the frame, it sets $c = c+1$, if it receives the same packet again.
- *Termination condition:* In the case where the successfully communicated packet is $m = M$, i.e, the last packet, a TX transmits the termination notification and terminates and an RX terminates upon receiving the terminate notification.

B Motivation for Adapt-R

a) Rationale for mode 1 and mode 2:

- Initially, a TX/RX pair operates in mode 1. When only legitimate competing TX/RX pairs are operating, mode 1 allows each TX/RX pair to communicate successfully in a frame with high probability, as any TX/RX pair not experiencing a collision does not perform random selection of a time slot in the next frame. This reduces the number of randomizing TX/RX pairs and also reduces the likelihood of collision among the TX/RX pairs which in turn reduces energy cost and increases the probability of success.

- When a reactive adversary is present, it can easily jam the communication of the TX/RX pair operating in mode 1 by deploying the following sequential attack strategy. It listens sequentially in each time slot of a frame, if it detects the transmission by the TX, it jams. It is easy to see that this reactive adversary can completely corrupt the communication of $(M-1)$ packets, as the TX will keep re-sending the first packet because the ACK is not received by the TX, whereas the RX will keep receiving the same first packet.
- To avoid this and any other arbitrary selection of time slots for attack by the adversary, each TX and RX maintains a counter c that tracks its number of failures in communicating a particular data packet. If c is greater than this threshold value T, it infers there is an adversary present. The TX/RX then operates in mode 2 of the protocol.
- In mode 2, the TX selects v_T time slots in a frame and transmits in each time slot with probability $\frac{1}{v_T}$, and stops if it receives an ACK from its intended RX. The RX listens sequentially in each time slot with probability $1/v_R$. The values of v_T and v_R are increased based on the number of unsuccessful communication attempts until they reach the value of s, at which it is kept constant. When $v_T, v_R = s$, i.e., the maximum value of v_T and v_R, on average the TX still transmits once in a frame, while the RX is now active only once per frame. However, for the adversary to completely block the communication with probability one, it needs now to be active in every time slot of the frame for which it will incur higher energy costs as compared to the TX and the RX. In short, the purpose of increasing v_T and v_R is to make the adversary incur more energy cost.
- Note that when a data packet is successfully communicated, the values of c and v_T are reset to 0 and 1, respectively. Hence, for every data packet, a TX and an RX first try to communicate in mode 1 and if it is not successful in c communication attempts then it operates in mode 2.

b) Rationale for RX listening sequentially:

In a frame, a transmitter (TX) changes the number of selected time slots and the access probability in each selected time slot based on the number of unsuccessful transmissions of a packet. When a TX transmits, from its receiver's (RX's) point of view, there are three possibilities when it listens in a time slot of a given frame: 1) It does not receive any data packet from the TX. In this case the RX continues listening in the next time slots of the frame with probability $1/v_R$ as there is a possibility that it might receive in some other time slot. 2) The RX receives the same data packet m again due to a lost ACK, for instance because the ACK was jammed. In this case the RX continues listening in the next time slots of the frame with probability $1/v_R$. 3) It receives a new data packet from the TX, i.e., a new data packet $m+1$ which was not received before. In this case the RX stops listening once it has sent an ACK. The RX then waits until the next frame. In the next frame the TX transmits and the RX listens in the same time slot in which a new packet was received. This allows the possibility that both the TX and the RX can save energy by operating in the same time slot for the communication of the next data packet.

c) Rationale for termination condition:

When all M data packets are successfully communicated, a termination condition for the TX/RX pair is important as otherwise the adversary may keep the TX/RX pair active for longer number of frames and hence can force it to incur a higher cost. For instance, consider the case where a TX transmits the last data packet $m = M$ and its RX successfully receives the packet. However, the adversary listens and jams the part of the time slot reserved for the ACK. If the RX after receiving the data packet and sending the ACK terminates, then the TX has no way of knowing whether the last data packet was communicated successfully. To avoid such a problem, when the RX successfully receives the last packet $m = M$, it transmits the ACK and then listens for *Terminate notification* from the TX in the same time slot. This ensures successful termination which we justify as follows. If the packet M is disrupted, then the TX knows not to terminate as the TX will not receive the ACK, and the RX knows not to terminate as it will not receive the data packet M. If the ACK is disrupted, i.e, the adversary listens for the data packet and then jams the part of the time slot reserved for the ACK, then both the TX and the RX will know because the TX will not receive the ACK and the RX will not receive the terminate notification. Note that jamming only the terminate notification is difficult for the adversary as it does not know whether the communicated data packet is the last data packet M or any other. Also, the terminate notification and the ACK are small packets, in practice, it is difficult for the adversary to distinguish between them [33, 38].

d) Choosing the threshold value T:

A threshold T is utilized by each TX and RX to decide whether to operate in mode 1 or mode 2. We propose that the nodes utilize the threshold value $T = \lceil (1/e^{(-N/s)}) \rceil$ for the decision. While we make no claims as to the optimality of the selected value of T, we justify it as follows: Consider the case where a TX has a data packet to communicate and the other $N-1$ competing TXs randomly with uniform distribution select a time slot out of s time slots in the frame. The probability of success in the frame for the TX is $(1-1/s)^{N-1}$. When only legitimate TXs are competing and when they randomly with uniform distribution select a time slot, it will take $(1-1/s)^{1-N}$ frames in expectation to transmit the data packet successfully. Hence, we suggest that the TX observes the number of unsuccessful attempts by maintaining the counter c and if c is greater than this threshold value T, it infers that there is an adversary present.

In the next section, we present benchmarking results by evaluating and comparing the effectiveness of the proposed method with the two other framed slotted Aloha-based approaches.

V Analytical and Numerical Performance Analysis of the Adapt-R Method

In this section, we first present analytical results for the proposed method. We then explain the two methods that are used to compare the performance of the proposed

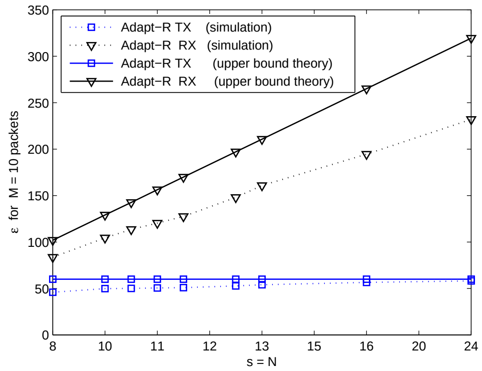


Fig. 4: Theoretical upper bound and simulated average cost of communication for $M = 10$ packets as a function of s time slots. $s = N$ competing TX/RX pairs and the cost of a transmission S and a listening L in a time slot are set to $S = L = 1$ unit.

method. We also present comparison results. Finally, we present extensive numerical results relating to the performance of the proposed method under different network scenarios.

A Analytical analysis of communications under competition

We first evaluate our proposed method under the scenarios where all TX/RX pairs are legitimate and compete with one another to access the channel. In this context, it is important not only to investigate the success rates of TX/RX pairs in a frame but also to investigate the rate at which TX/RX pairs attempt to communicate data packets, as more communication attempts mean more energy expenditure. In this context, useful measure of performance analysis is what are energy costs for each TX/RX pair to successfully communicate M data packets.

Next we provide an analytical result for the expected energy cost to communicate M packets under competition when $N \leq s$. Note that in Section V-E we also evaluate the performance of the proposed method when $N > s$.

Proposition 1 *Using the proposed method, the expected energy cost for a TX and an RX to communicate M data packets is not more than* $TM(S+L)$*, and* $TM\big((\frac{(s+1)}{2})L+S\big)$*, respectively, where* $T = \lceil 1/e^{\frac{N}{s}} \rceil$*, and* $N \leq s$ *is the number of competing legitimate TX/RX pairs.*

Proof See Appendix A.

For different values of $s = N$ time slots, in Fig. 4, we plot the theoretical upper bound presented in Proposition 5.1 and compare it with simulated average cost for successful communication of $M = 10$ data packets as a function of $s = N$ time slots. Observe that for the TX side the presented upper bound becomes tight with increasing $s = N$, while for the RX side it becomes loose with increasing $s = N$. This is due to the reason that for the RX side the upper bound considers the worst case scenario that in a frame the RX incurs always the maximum expected cost of $(\frac{(s+1)}{2}L + S)$.

B Analytical analysis of communications under conflict

In this subsection, we first consider the scenarios where a single TX is communicating to its intended RX and a reactive adversary tries to jam them. Then we consider the scenario where $N > 1$ TX/Rx pairs are communicating in the presence of a reactive adversary, i.e, we take into account both competition and conflict to evaluate the performance of the proposed method.

It is important to note that when an adversary has infinite amount of energy it can simply transmit in every time slot and jam all communication. However, such assumption is unlikely to hold in distributed networks. In our model, we consider the case where a legitimate TX, RX and an adversary has the same budget B units of energy, where B is sufficiently large. For simplicity of theoretical analysis we consider that $S = J$, i.e., the cost to transmit in a time slot is equal to the cost of jamming in a time slot. Moreover, when an adversary listens in a time slot for a data packet, it incurs the same cost L as incurred by a legitimate RX. However, in Section V-D, we also present results that take into account the effect of unequal energy costs for transmission, listening and jamming.

Before presenting the results, we briefly summarize the following observations:

Remark 1 The attack strategy where in each frame the adversary utilizes $s_J = s$ time slots for attack cannot be an energy efficient strategy for the adversary: The reason for this is as follows. The adversary with an energy budget B can completely block communication in not more than B/s frames, as it will completely deplete its energy after B/s frames. However, the TX will still have

$$B - \frac{B}{s}(S+L)$$

units of energy left and the RX will still have at least

$$B - \frac{B}{s}\left(\frac{(s+1)}{2}L + S\right)$$

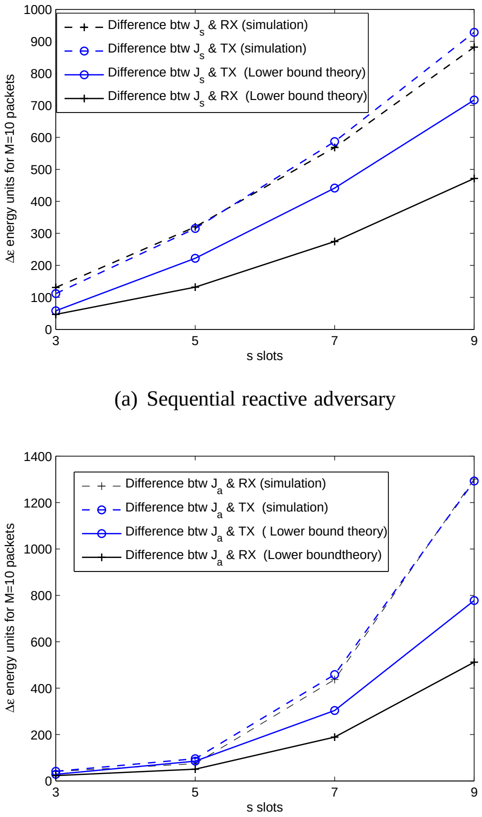
units of energy left. Moreover, expected total energy cost to communicate M data packets successfully for the TX is

$$\left(\frac{B}{s} + M\right)(S+L)\,\text{units}$$

and the expected total cost for the RX is not more than

$$\frac{B}{s}\left(\frac{(s+1)}{2}L + S\right) + M(S+L)\,\text{units}$$

.



(a) Sequential reactive adversary

(b) Arbitrary reactive adversary

Fig. 5: Theoretical lower bounds (presented in Proposition 5.4) and simulated differences in average cost between the adversary and a TX/RX pair as a function of time slots. The number of total packets that are successfully communicated are $M = 10$ and the cost of a transmission S, a listening L and a Jamming J in a time slot are set to $S = L = J = 1$ unit. Arbitrary reactive adversary selects $\lfloor s/2+1 \rfloor$ time slots in a frame.

Proposition 2 *When a TX wants to communicate M data packets to its intended RX then under the reactive jamming attacks the proposed method guarantees the communication of the M data packets with probability one.*

Proof See Appendix B.

Proposition 3 *For the proposed method, the expected number of frames to successfully communicate M data packets in the presence of a sequential reactive adversary is less than* $M(\frac{1}{P[S_c|J_s,v_T=v_R=s]}+T)$, *where* $T = \lceil 1/e^{\frac{N}{s}} \rceil$ *and* $P[S \mid J_s, v_T = v_R = s]$ *is the probability of successful communication in a frame when* $v_T = v_R = s$. *Moreover, expected number of frames* $E[N_F]$ *to transmit M data packets successfully in* *the presence of an arbitrary jammer adversary is less than* $\frac{M}{P[S_c|J_a, v_T = v_R = s]}$*, where* $P[S_c \mid J_a, v_T = v_R = s]$ *is the probability of successful communication in a frame when* $v_T = v_R = s$.

Proof See Appendix C.

Next, we show that the expected cost incurred by a TX *i* and its intended RX *i* to communicate *M* data packets is less than the cost incurred by the sequential or arbitrary reactive adversary who tries to block communication of the *M* packets. Moreover, the longer it takes a TX *i* and its intended RX *i* to successfully communicate the *M* data packets the more is the difference between the energy cost incurred by the adversary and the TX/RX. To derive the proof of less energy costs incurred by the legitimate TX and RX, for arbitrary reactive adversary, we assume that the adversary selects at least half of the time slots in a frame for launching attacks. Note that for the scenarios where adversary selects less than half of the time slots in a frame it may spend less energy in a frame. However, the probability of successful communication among the legitimate nodes increases as well.

Proposition 4 *In the presence of the sequential reactive adversary or the arbitrary reactive adversary which listens in at least half of the time slots in a frame, the expected cost to communicate M packets successfully for a TX is at least* $ME[N_F](\frac{s}{2} - 1)L$ *less than the jammer and the expected cost to its RX is at least* $ME[N_F](\frac{s}{2} - \ln s)L$ *less than the jammer, where* $E[N_F]$ *is the expected number of frames to successfully communicate a data packet.*

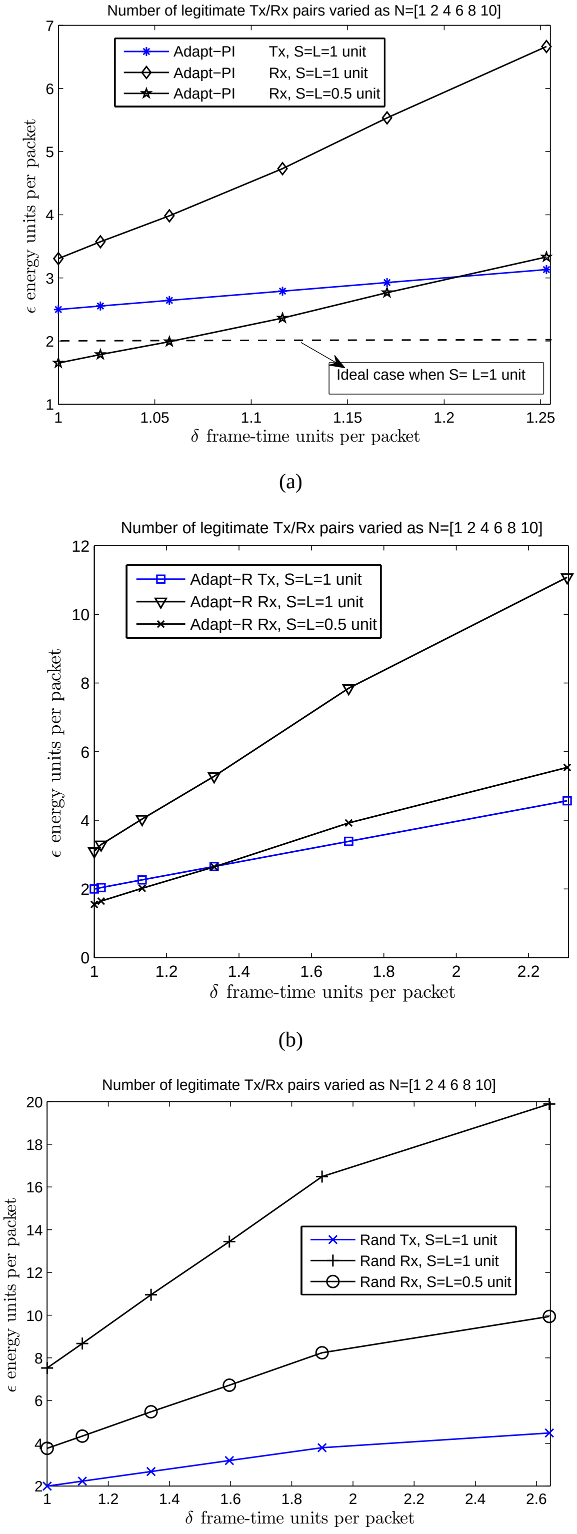
Proof See Appendix D.

For different values of *s* time slots in a frame, in Figs. 5a and 5b, we plot the theoretical lower bounds presented in Proposition 5.4 and compare them with simulated average differences between the cost incurred by the adversary and the legitimate TX and its RX, respectively.

Next we present some benchmarking results by evaluating and comparing the effectiveness of the proposed approach with two different approaches: 1) Adaptive framed slotted Aloha method with perfect information (Adapt-PI), where each TX/RX pair has *perfect information* in the sense that at the end of each frame each TX/RX pair has full knowledge of the time slot selections of other TX/RX pairs. 2) Random framed slotted Aloha method.

C Comparison with the Adapt-PI, Adapt-S and the Random framed-slotted Aloha methods

In the Adapt-PI method, at the end of each frame, it is considered that each TX/RX pair has full knowledge of the time slot selections of other TX/RX pairs, which allows the TX/RX pairs to minimize the likelihood of collisions with one another under competition, and also to minimize the likelihood of collisions under adversarial attacks.



(a)

(b)

(c)

Fig. 6: ε vs δ when N TX/RX pairs compete with one another. Number of TX/RX pairs is varied as 1, 2, 4, 6, 8 and 10, $s = 10$ time slots are available for access in each frame.

- Step 1: A TX begins by randomly with uniform probability choosing a time slot out of s time slots in a frame. It transmits a packet in the time slot and then listens for ACK. On the RX side, a RX sequentially listens in every time slot. It stops listening if it receives a packet from its intended TX and sends an ACK.
- Step 2: At the end of the frame, each TX/RX pair has perfect information about the time slot selections of all other TXs.
- Step 3: When no other TX selected the same time slot as the TX i, the TX i and its intended RX i selects the same time slot in the next frame for communication. Otherwise, the TX randomly selects a time slot out of those time slots that were not selected by any TX or that were selected by two or more transmitters in the previous frame. The RX sequentially listens in every time slot that was not selected by any TX or that was selected by two or more transmitters in the previous frame. It stops listening in that frame if it receives a packet from its intended TX.
- Step 4: If M packets have been successfully communicated then the TX/RX pair terminates; otherwise, go to Step 2.

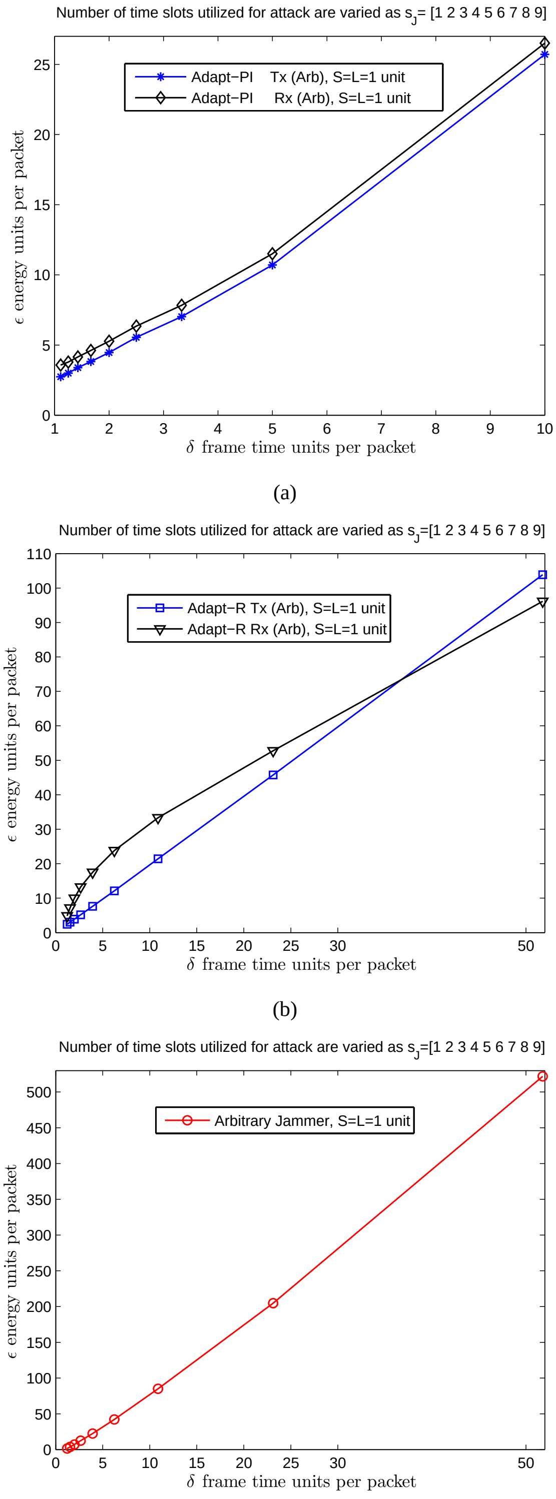
In the *random framed slotted Aloha-based method*, each TX randomly with uniform probability selects a time slot out of s time slots in a frame. It transmits a packet in the selected time slot and then listens for ACK from its intended receiver. On the RX side, each RX sequentially listens in every time slot. It stops listening when it receives a data packet from its intended TX and then it sends an ACK. In each frame the process is repeated and after successfully communicating the M data packets, both the TX and the RX terminate.

Before we present comparison of the results for the three methods, we briefly summarize some overall observations:

Remark 2 Under competition, in the ideal case where each TX/RX finds conflict-free allocations in the first frame then for $N = s$ TX/Rx pairs in the network, the energy cost to successfully communicate a data packet for each TX and RX is $(S+L)$ units.

Remark 3 Under competition, in the ideal case where each TX/RX pair finds conflict-free allocations in the first frame then for $N = s$ TX/RX pairs in the network, minimum delay incurred by a TX/RX pair to successfully communicate a packet is one frame-time unit as each TX/RX pair can successfully communicate once in every frame. A frame-time unit is the normalized duration of a frame with s time slots. When $N > s$, average delay incurred by a TX/RX pair is N/s frame-time units, as on average each TX/RX pair now requires more than one frame to successfully communicate a packet.

Let ε energy units represent the average energy cost to successfully communicate a data packet, and let δ frame-time unit be the delay cost incurred during this process. In Figs. 6a-6c, we present ε vs δ for a TX i and its intended RX i under the scenarios where the number of legitimate TX/RX pairs in the network is varied from 1 to $N = s$. In Figs. 6a-6c, we consider two different scenarios in terms of energy costs: 1) When all energy costs are considered to be equal, i.e., the cost of a transmission S, and a listening L in a time slot are normalized to $S = L = 1$ unit. Moreover, in the Adapt-PI method case the cost of sending time slot selection information and receiving



(a)

(b)

(c)

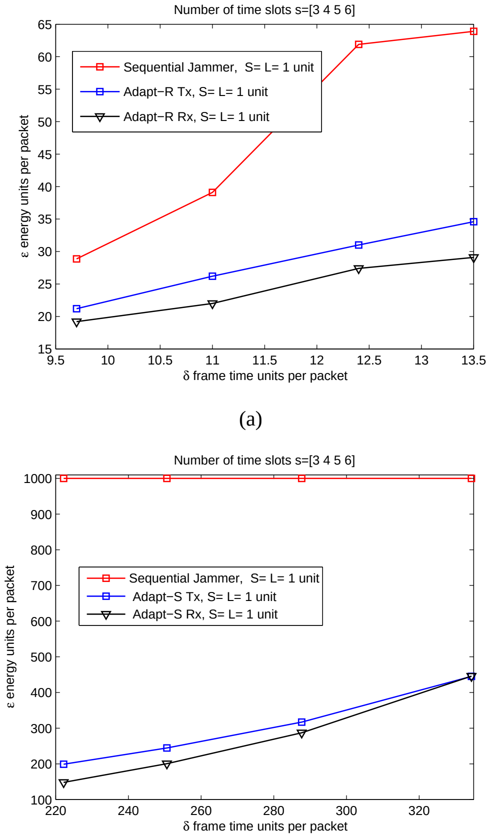
Fig. 7: ε vs δ when a TX/RX pair communicates in the presence of a reactive adversary. $s = 10$ time slots are available for access in each frame. Number of time slots s_J utilized for attack by the reactive arbitrary jammer is varied as $[1,2,3,4,5,6,7,8,9]$, and the cost of jamming J in a time slot is set to $J = S$ unit.

time slot selection vector-signal is set to $S = L = J = 0.5$ unit; and 2) When the energy costs incurred by a TX and an RX are considered to be different. This takes into account the scenarios in which there are lower costs for a receiving node as compared to a transmitting node. For instance, this can be due to transmission of a shorter duration of ACK as compared to a full data packet, and also due to lower cost for reception of a data packet as compared to its transmission. In this case, the energy cost of a transmission S and a listening L in a time slot incurred by an RX are considered to be half that of a TX, i.e., $S = L = 0.5$ unit.

It can be seen from Figs. 6a and 6b that when only multiple legitimate competing TX/RX pairs are present in the network then in terms of delay the proposed Adapt-R method performs close to both the ideal case and Adapt-PI methods. For the difficult scenario when $N = s = 10$, the Adapt-PI method takes 1.25 frame time units to communicate a packet successfully whereas the proposed Adapt-R method takes 2.2 frame time units to communicate a packet successfully. It can be also seen from Figs. 6a and 6b that in terms of energy costs, for the TX side, the proposed Adapt-R method once again performs close to both the ideal case and the Adapt-PI method. For the RX side, there is slight degradation in performance as compared to the Adapt-PI method when the numbers of competing TX/RX pairs is increased. However, it is important to note that the Adapt-PI method has significant advantage over the proposed distributed method as the TX/RX pairs in the Adapt-PI method have access to a secret channel in which they can share their time slot selection information. It can be also seen from Figs. 6b and 6c that the proposed method outperforms the random framed slotted Aloha method in terms of both energy and delay.

In Figs. 7a-7b, we present ε vs δ for a TX/RX pair under the scenarios where the number of time slots s_J utilized for attack by the reactive arbitrary jammer is varied from 1 to $(s-1)$. In Fig. 7c, we present the average energy cost incurred by the reactive arbitrary jammer for the same scenarios as considered in Figs. 7a and 7b. It can be seen from Figs 7b and 7c that to successfully communicate a packet a TX/RX pair incurs around 5 times less energy cost that of the reactive jammer. Moreover, the two figures also show that as the number of time slots utilized for attack by the jammer increases it takes longer for a TX/RX pair to successfully communicate. However, the more the jammer attacks the greater is the difference between the cost incurred by the adversary and the legitimate TX/RX. Hence, as a consequence the jammer will deplete its energy and a TX/RX pair can communicate its remaining packets efficiently.

The two figures in 7a and 7b show that for $s_J \leq 6$ the proposed method performs close to the Adapt-PI method, however, as the jammer utilizes $s_J > 6$ time slots for attack then the performance of the proposed method degrades as compared to the Adapt-PI method. When the jammer selects $s_J = 9$ time slots for attacks in every frame, the proposed method incurs 5 times larger delay than that of the Adapt-PI method and it incurs 4 times more energy cost than that of the Adapt-PI method. This is due to the reason that a TX/RX pair in the Adapt-PI method knows the time slot selections of the other legitimate TX/RX pairs. A TX/RX pair can use this information to distinguish whether a collision is caused because of time slot selection of other competing TX/RX pairs or due to a jamming attack. The time slot selection information of the other competing TX/RX pairs gives significant advantage to the



(a)

(b)

Fig. 8: Costs in terms of ε energy units per packet as a function of δ frame-time units per packet for different scenarios when $N = 1$ TR/RX pair communicate. In a) the results for a TX, RX and the jammer are given for the proposed Adapt-R method when the jammer uses the sequential jamming. In b) the results for a TX, RX and the jammer are given for the compared Adapt-S method when the jammer uses the sequential jamming. The cost of a transmission S, a listening L and a Jamming J in a time slot are set to $S = L = J = 1$ unit.

Adapt-PI method as compared to the proposed autonomous method in which TX/RX pairs have no access to a secret channel for time selection information exchanged between the TX and RX. In reality TX/RX pairs operating in an autonomous network cannot discern on its own whether communication failure is caused by other competing node or by an adversarial disruption. However, the Adapt-PI method provides a good baseline, so we can compare our proposed method with it.

For the performance of the random framed-slotted Aloha method under reactive jamming attack, we briefly summarize the following observation.

Remark 4 When the random framed slotted Aloha method is deployed for communication by a TX/RX pair in the presence of a reactive jamming adversary, the reactive

Table I: Costs in terms of ε energy units per packet when $N = 6$ TR/RX pairs compete under the different scenarios. $s = 6$ time slots are in a frame, $M = 10 packets$ and the cost of a transmission S, a listening L and a Jamming J in a time slot are set to $S = L = J = 1$ unit. The arbitrary jammer selects $s_J = 4$ time slots in each frame for the jamming attack.

	Sequential Jammer	Tx	Rx
ε (Adapt-R)	23.1	18.5	13.1
ε (Adapt-S)	206.6	129.6	94.9
	Arbitrary Jammer	Tx	Rx
ε (Adapt-R)	128.6	40.4	40.4
ε (Adapt-S)	87	32	36
	No Jammer	Tx	Rx
ε (Adapt-R)		6.9	4.84
ε (Adapt-S)		7	5.1

jammer can completely block the communication of $M-1$ out of M packets and can also make the RX completely depletes its energy by using the sequential jamming strategy in each frame. This is due to the reason that under the random framed slotted Aloha method the RX listens in every time slot of a frame until it receives a packet. The jammer using the sequential jamming strategy can also listen in every time slot of a frame until it detects the transmission which it then jams. By spending the same amount of energy as the RX, the jammer can completely block the communication of the RX. As the RX can only receive the first packet successfully, the TX keeps re-sending the first packet as an ACK is not received because of jamming.

In our work, we also compare the performance of the proposed method with another distributed approach which we call adaptive selection (Adapt-S) method. The Adapt-S method is given as follows:

- TX side: Select one time slot uniformly at random for transmission every time an ACK is not received
- RX side: If a packet is not received where expected (i.e., in the same time slot where a packet was received in the previous frame), then keep listening there for X more frames (where X is a random number which takes any value from 1 to s). If still not received, then listen everywhere (across the frame).
- Termination condition: In the case where the successfully communicated packet is $m = M$, i.e, the last packet, a TX transmits the termination notification and terminates and an RX terminates upon receiving the terminate notification.

In Fig. 8a-8b, we evaluate and compare ε vs δ performance of the proposed Adapt-R method with the Adapt-S method under the scenario where the jammer uses sequential jamming strategy. A frame-time unit δ is the normalized duration of a frame with s time slots. The number of time slots in a frame are varied as $s = [3, 4, 5, 6]$. It can be seen that under the sequential jamming attacks the proposed method significantly out performs the Adapt-S method. this is due to the reason that under the Adapt-S strategy the TR/Rx pair cannot communicate successfully until the sequential jammer does not completely deplete its own total energy budget of B units.

Table II: Average total energy cost per successful communication of a packet and average number of frames required to successfully communicate a packet for different number of time slots. In all scenarios the TX/RX pair communicate in the presence of a reactive sequential jammer J_s or reactive arbitrary jammer J_a.

	$s = 3, N = 1, M = 10$	$s = 5, N = 1, M = 10$	$s = 7, N = 1, M = 10$
Scenario 1:		$S = L = J = 1$ unit	
ε_{TX} under J_s, J_a	20.82, 8.8	25.2, 8.852	29.449, 18.55
ε_{RX} under J_s, J_a	21.881, 10.578	30.095, 13.044	38.48, 18.1
ε_{J_s}, ε_{J_a} under J_s, J_a	31.104, 12.14	52.7045, 16.7125	78.846, 39.423
Scenario 2		$S_d = 1$, $L_d = 0.5$, $L_{ack} = 0.25$, $J = 0.5$, $S_{ack} = 0.25$	
ε_{TX} under J_s, J_a	13.15, 5.6	15.8, 5.65	9.781, 6.1125
ε_{RX} under J_s, J_a	8.25, 5.175	14.0, 5.638	15.987, 7.46
ε_{J_s}, ε_{J_a}	15.752, 6.05	26.275, 8.36	23.383, 11.7
Scenario 3		Average number of frames to successfully communicate a packet	
Under J_s, J_a	10.6, 4.53	12.7, 4.6	14.8, 5.04

It is easy to see that the sequential adversary can completely block the communication of data packets until it completely depletes its energy budget (as the transmitter will keep re-sending the first data packet as ACK is not received, whereas the receiver will keep receiving the same first data packet). However, as under the Adapt-S method both the TR and the RX spend less energy in each frame as compared to the sequential jammer (when it is active), the TR/RX pair can still communicate the M packets once the adversary completely depletes its energy resources, however, they incur more delay. For example, when there are $s = 6$ time slots in a frame, the TR/RX requires $\delta = 320$ per packet for the Adapt-S, whereas the proposed method requires $\delta = 13.5$ per packet.

In Table I, we compare the performance of the proposed method with the Adapt-S method under the scenarios: a) $N = 6$ TR/RX pairs compete for access under the sequential jamming attacks, b) $N = 6$ TR/RX pairs compete for access under the sequential jamming attacks, and c) $N = 6$ TR/RX pairs compete and no jammer is present in the network. It can be seen from the results in the table that under the sequential jamming attacks the proposed method performs significantly well, under no jamming both the methods perform equally well, and under the arbitrary jamming the Adapt-S method performs better than the Adapt-R method. However, the difference in performance of the two methods under arbitrary jamming is less as compared to the difference in performance under the sequential jamming where the Adapt-R method performs significantly well.

Next we conduct extensive simulations to evaluate the performance of the proposed method under competition and conflict for different scenarios. Note that the simulations have been performed on different numbers of autonomous TX/RX pairs that form a fully connected interference graph.

Table III: Costs in terms of ε energy units per (successfully communicated) packet incurred by a TR, RX, and the jammer. The number of time slots s in a frame is 6 and the number of TX/RX pairs N is varied. The cost of a transmission S and Jamming J, are set to $S = J = 1$ unit whereas the cost of listening are set to $L = 1.5$ unit. The arbitrary jammer selects $s_J = 4$ time slots in each frame for the jamming attack.

	Sequential Jammer	TX	RX
ε when $N = 1$ (Adapt-R)	946.2	346.4	489.4
ε when $N = 2$ (Adapt-R)	415.5	167.5	256.2
ε when $N = 3$ (Adapt-R)	343.1	142.97	219.6
	Arbitrary Jammer	TX	RX
ε when $N = 1$ (Adapt-R)	416.5	151.5	250.8
ε when $N = 2$ (Adapt-R)	619.34	213.2	307.9
ε when $N = 3$ (Adapt-R)	760.5	248.6	332.3

D Numerical analysis of effect of varying energy cost

In Table II, we present the average energy cost incurred by a TX/RX pair to successfully communicate a data packet and also the average cost incurred by a reactive sequential jammer J_s and a reactive arbitrary jammer J_a that jams during the communication process. We consider two different scenarios: 1) When all costs are considered to be equal, i.e., the cost of a transmission S, a listening L and jamming J in a time slot are set to $S = L = J = 1$ unit; and 2) When the cost of sending, receiving and jamming are different, moreover, the cost of sending and receiving data is also different from the cost of sending and receiving an ACK. The cost of a transmission of a data packet is set to $S_d = 1$ unit, the cost of listening for a data packet for a legitimate node RX i or a jammer J is set to $L_d = 0.5$ unit, the cost of transmitting an ACK is set to $S_{ack} = 0.25$ unit, the cost of listening for an ACK is set to $L_{ack} = 0.25$ unit, and the cost of jamming is set to $J = 0.5$ unit. In Table II, we also present average number of frames required to successfully communicate a data packet in the presence of a jammer. It can be also seen from Table II that the jammer incurs higher average energy cost for all the scenarios as compared to the legitimate nodes. Moreover, it can be also seen that as the number of time slots in a frame is increased, the average cost incurred by the jammer is significantly increased as compared to the legitimate TX and RX nodes.

It is possible that in the Machine-to-Machine (M2M) networks, many M2M devices consume more energy while in receiving mode as compared to when in the transmit mode. To take this into account, in Table III, we provide results for the case where the normalized energy costs for listening are more as compared to transmitting and jamming. In Table III, we present ε for a TR, an RX, the sequential jammer, and the arbitrary jammer under the scenario where the number of TR/RX is varied, and the cost for listening is 50% more than the cost of transmission and jamming. It can be seen that similar to the results presented in Figs 5-10 and Tables I-II, a legitimate TR and its intended RX consume less energy than the jammer for all scenarios. hence, our designed protocol ensures that it is significantly more costly for a reactive adversary to disrupt communications than for a TX and an RX node to communicate. In other words, our protocol forces the energy-constraint adversary to incur higher en-

Table IV: Average cost and average number of frames to communicate a data packet. The number of time slots s in a frame is 10 and the number of TX/RX pairs is $N > s$. The cost of a transmission S and a listening L in a time slot are set to $S = L = 1$ unit.

	$N = 12$	$N = 14$	$N = 16$
ε_{TX}	7.13	8.96	13.32
ε_{RX}	14.26	18.48	23.8
Average number of frames	3.59	4.51	6.73

ergy cost relative to an energy constraint legitimate node and guarantees successful communication of packets.

E Numerical analysis of effect of $N > s$:

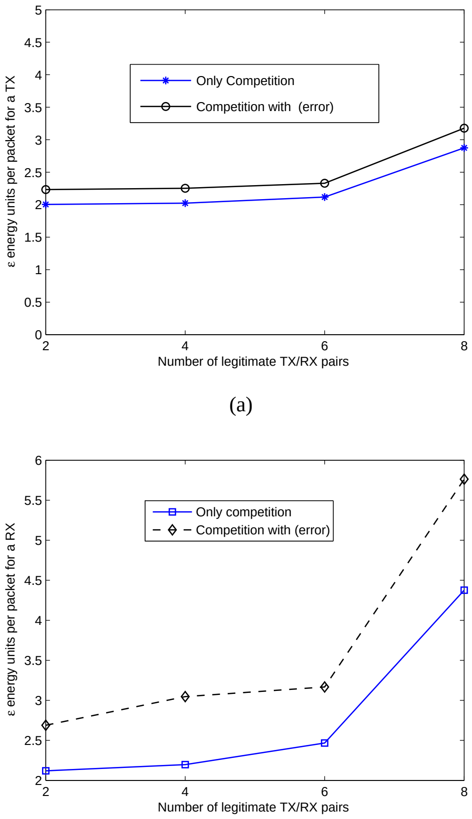
Table IV evaluates the scenarios where the number of autonomous TX/RX pairs is greater than the number of time slots in a frame. It can be seen from Table IV that as expected when N is increased then average cost in terms of energy and in terms of number of frames also increases for the legitimate TX and RX nodes.

F Numerical analysis of effect of channel error and capture effect:

In Figs. 9a and 9b, we evaluate and compare the average energy cost per successful communication of a data packet for the following scenarios. 1) Only competition: N legitimate TX/RX pairs compete to communicate their $M = 50$ data packets; and 2) Competition with errors: N legitimate TX/RX pairs compete to communicate their $M = 50$ data packets successfully in the presence of channel errors and capture effect. Analyzing a network in which N autonomous TX/RX pairs compete in the presence of imperfect channel observations is challenging due to the combinatorial explosion in the number of ways that a TX/RX pair can find a time slot free from the adversarial jamming and the other TX/RX pairs. To evaluate the effect of channel error and capture, for simplicity, we consider a probabilistic memoryless channel error and capture model. We use a model where when a TX transmits in a time slot then due to a channel error a packet is not successfully received by its intended RX with probability σ_e. Moreover, when two or more transmitters transmit simultaneously in the same time slot then with probability σ_t an RX can still successfully receive a packet due to capture effect. In the simulation analysis σ_e and σ_t are set to $\sigma_e = 0.1$ and $\sigma_t = 0.1$ respectively. It can be seen from the Figs. 9a and 9b that the average cost slightly increases with the increasing number of TX/RX pairs in the network and also when there are errors present in the network.

G Numerical analysis of performance in terms of average number of frames

In Fig. 10, we evaluate the effect of increasing number of N TX/RX pairs on the performance of the proposed protocol in terms of average number of frames required



(a)

(b)

Fig. 9: Average total energy cost per successful communication of packet as a function of N legitimate TX/RX pairs for different scenarios. $s = 10$ time slots are in a frame and the cost of a transmission S, a listening L and a Jamming J in a time slot are set to $S = L = J = 1$ unit. Arbitrary reactive adversary selects $s_J = 6$ time slots randomly for attack.

to successfully communicate a packet. We evaluate this performance under two different scenarios as explained in Section V-F and also under the following additional scenarios: a) Competition and sequential adversary: N legitimate TX/RX pairs compete to communicate their $M = 50$ packets successfully in the presence of a sequential reactive adversary; and b) Competition and arbitrary adversary: N legitimate TX/RX pairs compete to communicate their $M = 50$ packets successfully in the presence of an arbitrary reactive adversary. It can be seen from Fig. 10 that the presence of arbitrary reactive adversary requires more number of frames to successfully communicate a packet as compared to the other scenarios.

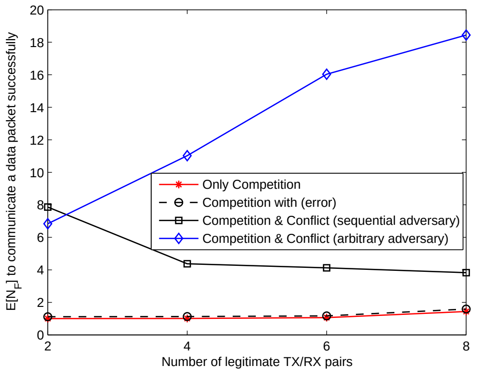


Fig. 10: Average number of frames to communicate a data packet successfully $(E[N_F])$ as a function of N legitimate TX/RX pairs for different scenarios. $s = 10$ time slots in a frame, the number of total data packets communicated are $M = 50$ and the cost of a transmission S, a listening L and a Jamming J in a time slot are set to $S = L = J = 1$ unit. Arbitrary reactive adversary selects $s_J = 6$ time slots randomly for attack.

VI Concluding Remarks

Due to new applications of distributed wireless networks, such as wireless machine-to-machine networks and wireless sensor networks, there has been increased interest in research on distributed protocols that enable secure co-existence among multiple energy-constrained nodes. In this paper, we investigate the problem of reliable communication of multiple data packets among energy constrained autonomous nodes, that are competing over a shared medium and may face adversarial disruptions. We propose a distributed method and show that it can guarantee reliable communication among the nodes in the presence of competition and it also reduces the probability of collisions among the competing nodes. We then evaluate the robustness of this protocol to unknown environmental conditions such as adversarial disruptions in communication. We consider scenarios where energy is a scarce resource for both the adversary and legitimate competing nodes. In this context, we consider a notion of relative cost in terms of energy. We show that when legitimate nodes use our method then it is significantly more costly for a reactive adversary to disrupt communications than for the nodes to communicate. We also present results comparing the effectiveness of the proposed method with two other approaches.

Acknowledgement

This work was funded by Academy of Finland under the grant number 268997

References

1. P. Huang, L. Xiao, S. Soltani, M. Mutka, and X. Ning, “The evolution of MAC protocols in wireless sensor networks: A survey,” *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 101–120, First 2013.
2. F. Vázquez-Gallego, L. Alonso, and J. Alonso-Zarate, “Modeling and analysis of reservation frame slotted-aloha in wireless machine-to-machine area networks for data collection,” *Sensors, Special Issue Wireless Sensor Networks and the Internet of Things*, vol. 15(2), pp. 3911–3931, Feb. 2015.
3. W. Jeon and D. Jeong, “Combined channel access and sensing in cognitive radio slotted-aloha networks,” *IEEE Transactions on Vehicular Technology*, To appear, 2015.
4. H. Okada, Y. Igarashi, and Y. Nakanishi, “Analysis and application of framed ALOHA channel in satellite packet switching networks-FADRA method,” *Electronics Communications of Japan*, vol. 60, pp. 72–80, 1977.
5. A. Munari, M. Heindlmaier, G. Liva, and M. Berioli, “The throughput of slotted aloha with diversity,” in *Proceedings of the 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, October 2013, pp. 698–706.
6. D. Bajovic, D. Jakovetic, D. Vukobratovic, and V. S. Crnojevic, “Slotted Aloha for networked base stations,” in *Proceedings of the IEEE International Conference on Communications Workshops (ICC)*, June 2014, pp. 520–526.
7. A. MacKenzie and S. Wicker, “Stability of multipacket slotted aloha with selfish users and perfect information,” in *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM)*, March 2003, pp. 1583–1590.
8. H. Wu, C. Zhu, R. La, X. Liu, and Y. Zhang, “Fasa: Accelerated s-aloha using access history for event-driven m2m communications,” *Networking, IEEE/ACM Transactions on*, vol. 21, no. 6, pp. 1904–1917, 2013.
9. W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc)*, December 2005, pp. 46–57.
10. M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, “Short paper: Reactive jamming in wireless networks: How realistic is the threat?” in *Proceedings of the Fourth ACM Conference on Wireless Network Security (WiSec)*, June 2011, pp. 47–52.
11. R. Raymond and S. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defenses,” *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.
12. A. Proano and L. Lazos, “Selective jamming attacks in wireless networks,” in *Proceedings of the IEEE International Conference on Communications (ICC)*, May 2010, pp. 1–6.
13. A. Richa, C. Scheideler, S. Schmid, and J. Zhang, “An efficient and fair mac protocol robust to reactive interference,” *IEEE/ACM Transactions on Networking*, vol. 21, no. 3, pp. 760–771, 2013.
14. K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *IEEE Communications Surveys Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.
15. R. Ma, V. Misra, and D. Rubenstein, “An analysis of generalized slotted-aloha protocols,” *IEEE/ACM Transactions on Networking*, vol. 17, no. 3, pp. 936–949, 2009.
16. Y. Law, M. Palaniswami, L. Hoesel, J. Doumen, P. Hartel, and P. Havinga, “Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols,” *ACM Transactions on Sensor Networks*, vol. 5, no. 1, February 2009.
17. M. Young and R. Boutaba, “Overcoming adversaries in sensor networks: A survey of theoretical models and algorithmic approaches for tolerating malicious interference,” *IEEE Communications Surveys Tutorials*, vol. 13, no. 4, pp. 617–641, 2011.
18. V. King, J. Saia, and M. Young, “Conflict on a communication channel,” in *Proceedings of the 30th annual symposium on Principles of distributed computing (PODC)*, June 2011, pp. 277–286.
19. S. D’Oro, L. Galluccio, G. Morabito, S. Palazzo, L. Chen, and F. Martignon, “Defeating jamming with the power of silence: a game-theoretic analysis,” *IEEE Transactions on Wireless Communications*, vol. to appear, 2015.
20. A. Boukerche and X. Li, “An agent-based trust and reputation management scheme for wireless sensor networks,” in *IEEE Global Telecommunications Conference, (GLOBECOM)*, vol. 3, 2005, pp. 1–5.
21. A. Boukerche and Y. Ren, “A secure mobile healthcare system using trust-based multicast scheme,” *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 387–399, 2009.
22. Y. Ren, R. Werner, N. Pazzi, and A. Boukerche, “Monitoring patients via a secure and mobile healthcare system,” *IEEE Wireless Communications*, vol. 17, no. 1, pp. 59–65, 2010.

23. A. Boukerche, X. Cheng, and J. Linus, “Energy-aware data-centric routing in microsensor networks,” in *Proceedings of the 6th ACM International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, ser. MSWIM ’03, 2003, pp. 42–49.
24. A. Boukerche, Ed., *Handbook of Algorithms for Wireless Networking and Mobile Computing*. CRC Press, Taylor and Francis Group, 2005.
25. J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, and Y. Qiao, “A survey on position-based routing for vehicular ad hoc networks,” *Telecommunication Systems*, vol. 62, no. 1, pp. 15–30, 2015.
26. M. Chen, J. Wan, S. Gonzalez, X. Liao, and V. C. M. Leung, “A Survey of Recent Developments in Home M2M Networks,” *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 98–114, 2014.
27. X. Li, D. Li, J. Wan, A. V. Vasilakos, C.-F. Lai, and S. Wang, “A review of industrial wireless networks in the context of Industry 4.0,” *Wireless Networks*, pp. 1–19, 2015.
28. C. Floerkemeier, “Bayesian transmission strategy for framed ALOHA based RFID protocols,” in *Proceedings of the IEEE International Conference on RFID*, March 2007.
29. M. Fang, D. Malone, K. R. Duffy, and D. J. Leith, “Decentralised learning MACs for collision-free access in WLANs,” Sep. 2010. [Online]. Available: http://arxiv.org/abs/1009.4386v1
30. R. L. Rivest, “Network control by bayesian broadcast,” *IEEE Transactions on Information Theory*, vol. 33, no. 3, pp. 323–328, 1987.
31. S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport, “Secure communication over radio channels,” in *Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing (PODC)*, August 2008, pp. 105–114.
32. M. Mohi, A. Movaghar, and P. Zadeh, “A bayesian game approach for preventing DoS attacks in wireless sensor networks,” in *Proceedings of the International Conference on Communications and Mobile Computing*, January 2009, pp. 507–511.
33. Z. Zhang, J. Wu, J. Deng, and M. Qiu, “Jamming ACK attack to wireless networks and a mitigation approach,” in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, November 2008, pp. 4966–4970.
34. J. Chen, S. Sen, M. Chiang, and D. Dorsey, “A framework for energy-efficient adaptive jamming of adversarial communications,” in *Proceedings of the 47th Annual Conference on Information Sciences and Systems (CISS)*, March 2013, pp. 1–6.
35. Y. Xiao and Y. Pan, *Emerging wireless LANs, wireless PANs, and wireless MANs: IEEE 802.11, IEEE 802.15, 802.16 wireless standard family*, ser. Wiley Series on Parallel and Distributed Computing. Hoboken, NJ: Wiley, 2009.
36. G. Linnenbank, “A power dissipation comparison of the R-TDMA and the slotted-aloha wireless MAC protocols,” Enschede, 1997, Moby Dick Project Report. [Online]. Available: http://doc.utwente.nl/20249/
37. G. Anastasi, M. Conti, M. Francesco, and A. Passarella, “Energy conservation in wireless sensor networks: A survey,” *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.
38. N. Sufyan, N. Saqib, and M. Zia, “Detection of jamming attacks in 802.11b wireless networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1–18, 2013.

A Proof of Proposition 1

Proof When $c \leq T$, a TX and its intended RX operate in mode 1, in which the TX selects a time slot randomly (with uniform distribution), transmits a data packet in the selected time slot, while its intended RX listens sequentially. It is easy to see that for N competing TX/RX pairs the probability of successful communication for each TX/RX pair in mode 1 is $(1-1/s)^{N-1}$, and the expected number of frames $E[N_F]$ required to communicate a data packet successfully is

$$E[N_F] = (1-1/s)^{1-N}. \tag{1}$$

This means that using the proposed method the average number of frames required to successfully communicate a data packet is not more than the threshold value $T = \lceil 1/e^{\frac{N}{s}} \rceil$, as $E[N_F] = (1-1/s)^{1-N}$ is less than or equal to the selected threshold value $T = \lceil 1/e^{\frac{N}{s}} \rceil$. For M packets this value is TM.

The expected energy cost for a TX and its intended RX to communicate a data packet successfully is not more than $(S+L)$ and $(\frac{(s+1)}{2}L+S)$ respectively. The reason is as follows: the TX transmits and listens on average once per frame, on average the RX listens in not more than $\left(\frac{(s+1)}{2}\right)$ time slots and on average it transmits ACK once per frame. Hence, using the proposed method, the expected energy cost for a TX and its intended RX to communicate M packets successfully is not more than $TM(S+L)$ units and $TM(\frac{(s+1)}{2}L+S)$ units respectively, this proves our claim.

B Proof of Proposition 2

Proof In a frame, the probability of a successful communication of a data packet in the presence of a sequential jammer (J_s) is

$$
\begin{aligned}
P[S_c \mid J_s] =& Pr\{\text{TX } i \text{ transmits in a time slot} \mid \text{TX } i \text{ has transmitted once before in a time slot in that frame}\} \\
& \times Pr\{\text{RX } i \text{ receives in that time slot}\}
\end{aligned} \tag{2}
$$

which is given by

$$
P[S_c \mid J_s] = \begin{cases} 0, & \text{if Mode 1} \\ \sum_{i=2}^{v_T} (\frac{1}{v_T})^i (\frac{1}{v_R})(1-\frac{1}{v_R})^{i-2} + & \\ \left[\sum_{i=2}^{v_T} \{ \binom{v_T}{i} - 1 \} (\frac{1}{v_T})^i (1-\frac{1}{v_T})^{v_T-i}\right] (\frac{1}{v_R})(1-\frac{1}{v_R})^{i-2}, & \text{otherwise} \end{cases} \tag{3}
$$

where $2 \leq v_T \leq s$. For example, when in mode 1 a TX selects only one time slot in a frame and transmits in it with probability one. In this case $P[S_c \mid J_s] = 0$, as the jammer by employing sequential jamming can jam this transmission with probability one. When the jammer employs the sequential jamming strategy, it sequentially listens in time slots until it detects a transmission, blocks the transmission and then waits for the next frame, so for $P[S_c \mid J_s] > 0$, the TX needs to transmit more than once in a frame. In other words it can only successfully transmit in mode 2, where $v_T \geq 2$ and the TX selects two or more time slots in a frame and transmits in each of them with probability $1/v_T$. Suppose that there are $s = 3$ time slots in every frame, in this case the TX and its intended RX can successfully communicate with $P[S_c \mid J_s] > 0$, when $v_T = 2$ or when $v_T = 3$. For $v_T = 2$, the TX selects two time slots in a frame and it transmits in each of them with probability $1/v_T$. The TX will be unsuccessful in the first transmission and can be successful in the second transmission if the RX listens in that time slot. In this case the probability of success obtained from Eq. (3) is: $(\frac{1}{v_T})(\frac{1}{v_T})(\frac{1}{v_R})$. For higher values of s and v_T, Eq (3) simply calculates the probability that in how many ways the TX and the RX can successfully communicate given that the TX selects v_T time slots in a frame and transmits in each of them with probability $1/v_T$ while the RX listens in every time slot with probability $1/v_R$.

In a frame, the probability of a successfull communication of a data packet in the presence of an arbitrary adversary (when the adversary picks $s_J > 0$ out of s time slots in a frame) is given by

$$
P[S_c \mid J_a] = \begin{cases} 0, & \text{if } s_J = s \\ \sum_{i=1}^{v_T-s_J} \left\{ P_{s,i} \prod_{j=1}^{i-1} (1-P_{s,j}) \right\}, & \text{if } v_T = s,\ 0 \leq s_J < s \\ \sum_{x=0}^{\min\{v_T, s_J\}} \left[\frac{\binom{v_T}{x}\binom{s-v_T}{s_J-x}}{\binom{s}{s_J}} \left\{ \sum_{i=1}^{v_T-x} P_{s,i} \prod_{j=1}^{i-1} (1-P_{s,j}) \right\} \right], & \text{otherwise} \end{cases} \tag{4}
$$

where $P_{s,i}$ is an element of the s-length vector $\mathbf{P}_s$. The vector $\mathbf{P}_s$ is given by $\mathbf{P}_s = [P_{s,1}, P_{s,2}, \cdots, P_{s,s}] = [\frac{1}{v_T}\frac{1}{v_R}, \frac{1}{v_T}\frac{1}{v_R}, \cdots, \frac{1}{v_T}\frac{1}{v_R}]$.

For example, in the frames where the adversary select $s_J = s$ slots for attack, i.e., it selects every slot in the frame, the probability of success is $P[S_c \mid J_a] = 0$. When the adversary randomly selects $s_J < s$ time slots in a frame for attack, a TX and its intended RX may successfully communicate in those time slots that are not selected by the adversary. To calculate the probability of success, we need to find the following: 1) The probability that x out of v_T time slots are selected by the adversary, where $x = 0, 1, \cdots, v_T$. The probability of this event happening is given as: $\left(\frac{\binom{v_T}{x}\binom{s-v_T}{s_J-x}}{\binom{s}{s_J}}\right)$; 2) In the $v_T - x$ remaining time slots which are not selected by the adversary, the probability that the TX will transmit and the RX will listen in the same slot is given as: $\sum_{i=1}^{v_T-x} P_{s,i} \prod_{j=1}^{i-1}(1-P_{s,j})$.

Let f_j represent a frame in which both $v_T > 1$ and $v_R > 1$ when the adversary employ sequential jamming attack, or let f_j represent a frame where $J_s < s$ when the adversary employ arbitrary jamming attack. Let P_j be the maximum probability that the packet will not be successfully communicated in a frame f_j. Note that for the considered scenario under sequential jamming attack, or for a given s_J under arbitrary jamming attack, maximum probability of unsuccessful communication P_j occurs when both $v_T = s$ and $v_R = s$. As with increasing v_T the TX in each of the v_T selected time slots, transmits with probability $1/s$, whereas with increasing value of v_R, the RX decreases the probability of listening in a time slot. Hence, $v_T = v_R = s$ corresponds to the situation in which the probability of successful communication is minimum in a frame. This probability can be calculated using Eq. 3 for sequential jamming scenario and using Eq. 4 for arbitrary jamming scenario. The probability of not being successfully communicated in n of such frames is less than or equal to $(P_j)^n$, in $2n$ frames is less than or equal to P_j^{2n}, etc. Since $P_j < 1$, these probabilities tend to zero. Hence, $\lim_{n\to\infty} P_j^n = 0$, which proves our claim.

C Proof of Proposition 3

Proof In the presence of a sequential reactive adversary, for each data packet, the probability of successful communication of a packet is zero in the first T frames where $c \leq T$. When $c > T$, it is easy to see (from Eq. 3) that for the proposed method, the probability that a data packet is successfully communicated in any frame is minimum when v_T and v_R reach their maximum value of s. As with increasing v_T a TX in each of the v_T selected time slots, transmits with probability $1/s$, whereas with increasing value of v_R, an RX decreases the probability of listening in a time slot. Hence, $v_T = v_R = s$ corresponds to the situation in which the probability of successful communication is minimum in a frame. Due to this reason, $P[S_c \mid J_s]$ in a frame is at least $P[S_c \mid J_s, v_T = v_R = s]$ and hence $E[N_F \mid J_s] < M(\frac{1}{P[S_c|J_s,v_T=v_R=s]} + T)$.

In the presence of an arbitrary reactive jammer, for a given s_J time slots used for attack in a frame, the conditional probability of successful communication is at least $P[S_c \mid J_a, v_T = v_R = s] = \frac{1}{s^2}\sum_{i=1}^{s-s_J}(1-\frac{1}{s^2})^{(i-1)}$. The conditional probability of success $P[S_c \mid J_a, v_T = v_R = s]$ corresponds to the worst case situation when v_T and v_R reach their maximum value of s. Hence for successful communication of the M data packets, $E[N_F \mid J_a] < \frac{M}{P[S_c|J_a,v_T=v_R=s]}$.

D Proof of Proposition 4

Proof Using the proposed method, a TX transmits and listens once per frame in expectation. Therefore, the average energy cost of the TX to successfully communicate M packets is $ME[N_F](S+L)$, where $E[N_F]$ is the average number of frames to successfully communicate a packet.

The arbitrary jammer that selects at least half of the time slots in a frame for attack has expected energy cost of at least $(\frac{s}{2})L + S$ per frame. Hence, the expected cost to communicate M packets successfully for the TX is at least $ME[N_F](\frac{s}{2} - 1)L$ less than the jammer.

When the adversary employs sequential jamming attacks, we first show the cost incurred in the frames where $c \leq T$. The expected cost for the sequential adversary in these frames is $\left(\frac{(s+1)}{2}L + S\right)$. This is due to the reason that in each frame the TX selects a time slot and transmits in it, while the adversary sequentially listens in time slots until it detects a transmission and blocks it.

In the frames where $c > T$, the TX instead of selecting a single time slot it changes the number of selected time slots ν_T, where $1 < \nu_T \leq s$. The expected cost per frame for the sequential adversary in this case is given by

$$E[C_{J_s}] = \sum_{L=1}^{s}(L+S)a_L + \big(1 - \sum_{L=1}^{s} a_L\big)L, \tag{5}$$

where

$$a_L = \sum_{k=1}^{v_T} W^k T_L^k,$$

$$W^k = (1 - \frac{1}{v_T})^{k-1}\frac{1}{v_T}$$

and

$$T_L^k = \begin{cases} \frac{\binom{L-1}{k-1}\binom{s-L}{v_T-k}}{\binom{s}{v_T}}, & \text{if} k \leq L \leq s - v_T + k \\ 0, & \text{otherwise.} \end{cases}$$

It can be calculated using Eq. 5 that for any $\nu_T > 1$, the average cost of sequential jammer is greater than or equal to $\left(\frac{(s+1)}{2}L + S\right)$. The reason is as follows: For $\nu_T > 1$, when the TX selects ν_T time slots and transmits in each of these time slots with probability $1/\nu_T$, the adversary now needs to listen (on average) in more than $\left(\frac{s+1}{2}\right)$ time slots to detect the transmission. Moreover, there is also now a possibility that the TX does not transmit in any time slots, in this case, the adversary incurs the maximum cost of sL in that frame. Hence the cost to adversary is at least $\left(\frac{(s+1)}{2}L + S\right)$. Due to this reason, the expected cost to communicate M packets successfully for the TX is at least $ME[N_F](\frac{s}{2} - 1)L$ less than the sequential jammer.

For the RX, when $c \leq T$ then $v_R = 1$ and the expected energy cost to the RX is $E[C_{RX} \mid c \leq T] = \left(\frac{(s+1)}{2}L + S\right)$, i.e., the same cost as incurred by the adversary. However, when $c > T$, the RX instead of listening with probability one in a time slot, listens with probability $1/\nu_R$, where $1 < \nu_R \leq s$. Hence the cost of the RX per frame decreases with increasing v_R. When $v_R = 2$, the expected cost of the RX in a frame is $\left(\frac{s}{2}L + S\right)$ and so on. Finally, when $v_R = s$, the expected cost for the RX in each of the remaining frames is $(S + L)$. It can be seen that the costs for the RX (when $v_R > 1$) are less than the costs incurred by the adversary. For $v_R > 2$, the total expected energy cost to the RX is given as

$$E[C_{RX} \mid v_R > 2] = \sum_{v=3}^{s} \frac{s}{v}L + (s-2)S. \tag{6}$$

Clearly, the expected cost in the frames where $v_R > 2$ is upper bounded by $(s-2)(S + L\ln s)$, i.e.,

$$E[C_{RX} \mid v_R > 2] < (s-2)(S + L\ln s)$$

whereas the expected cost of the jammer in these frames is at least $(s-2)(\frac{s}{2}L + S)$, as explained above. Due to this reason, the expected cost to communicate M packets successfully for the RX is at least $ME[N_F](\frac{s}{2} - \ln s)L$ less than the adversary, which proves our claim.