Design of a Joint Defense System for Mobile Ad Hoc Networks

Huei-Wen Ferng and Chien-Liang Liu
Department of Computer Science and Information Engineering
National Taiwan University of Science and Technology, Taipei 106, Taiwan
E-mail: hwferng@mail.ntust.edu.tw

***Abstract*— A mobile ad hoc network (MANET) is vulnerable to malicious attacks although it is suitable for various environments because of its rapid establishment. In order to set up a secured MANET, we should not only adopt encryption and authentication, but also equip each node with an intrusion detection system to detect malicious attackers. Focusing on intrusion detection, we propose an intrusion detection system that integrates a finite state machine (FSM) and a support vector machine (SVM) to analyze traffic patterns of MANETs. Shown by numerical examples, such an intrusion detection system is able to amend drawbacks of single-technique systems and enhance usage/right of normal users as well as security of MANETs.**

I. Introduction

A mobile ad hoc network, i.e., MANET, is a collection of mobile hosts that can communicate with each other without any pre-established infrastructure. Therefore, MANET has the property of rapid infrastructure-less deployment which makes it convenient to many environments, such as battlefields, conferences, or some emergency rescues. However, MANET is prone to malicious attacks [12], [15] due to the nature of mobile wireless networks. In [8], the authors have shown how these attacks affect the network.

In MANETs, AODV [11] is one of important routing protocols; however, no security mechanism has initially been specified for it. That is to say, no means protects the system against attacks to AODV, e.g., IP/MAC spoofing and packet discarding etc. Therefore, some new protocols have been proposed for this reason, e.g., SAR [17], SAODV [18], to strengthen the security of AODV based on the concept of encryption/decryption. However, the computational ability of a mobile device is often insufficient for a complicated encryption/decryption. Hence, these protocols may degrade system performance and enlarge packet delay. Moreover, only specific but not generic attacks can be identified by them. To further provide high survivability to a network, an intrusion detection system (IDS), e.g., those in [1], [7], is frequently employed as the second line of defense against attacks to conserve the integrity and confidentiality of the transmitted data and to provide the availability of network resources.

Although many mechanisms of IDS have been already proposed for wired networks, they are hard to be directly applied to wireless networks, in particular, MANETs. The reason why one cannot directly apply those protocols in wired networks to MANETs is the difference of infrastructure. In MANETs, no infrastructure nor a centralized audit point, e.g., gateway or router in the Internet, exists. Moreover, the distributed algorithm rather than the centralized one employed by those IDS systems in wired networks should be utilized in the design for the IDS system in MANETs. Therefore, Zhang and Lee [19] designed a distributed and cooperative architecture for IDS in the literature. In their proposed architecture, all mobile nodes are equipped with an IDS, called IDS agent with six components, i.e., local data collection, secure communication, local detection engine, cooperative detection engine, local response, and global response. In [5], Hijazi and Nasser applied the concept of *mobile agent* into the design of IDS. Bhargava and Agrawal [2] proposed a new architecture based on that in [19]. More specifically, they focused on IDS for AODV and proposed two models, i.e., intrusion detection model and intrusion response model. Using the threshold approach with the aid of a counter called *malcount*, they can detect malicious attacks. In [16], Vigna et al. proposed AODVSTAT for AODV based on the state transition analysis technique (STAT) which is originally designed for wired networks. AODVSTAT has two modes, i.e., stand-alone mode and distributed mode. Finally, Tseng et al. [13] proposed an architecture different from that in [19]. They only put an IDS to network monitor nodes rather than all mobile nodes and used three states to denote detection outcomes, i.e., normal, suspicious, and alarm.

All aforementioned papers can be categorized into IDS based on transitions of states, i.e., FSM, for known attacks. For unknown attacks, one is able to extract features from attacks and train a system to combat attacks, e.g., using SVM which was proposed by Vapnik [14] based on statistics learning theory. Of course, one can apply other theories to the design of IDS for MANETs, for example, Dempster-Shafer theory [3]. As far as AODV routing protocol is concerned, Zhang et al. [20] compared the traditional data mining approach called RIPPER with SVM and demonstrated the superior of SVM over RIPPER. In [4], Deng et al. proposed a two-stage IDS approach to detect attacks to AODV utilizing two SVMs, i.e., 1-SVMDM for the first stage and 2-SVMDM for the second stage. For an IDS system using SVM, it requires a longer time to train the system and is probably attacked before the system is ready to detect attacks. To get advantages of two approaches, i.e., FSM and SVM, so that the decision time is shortened and the detection scope is enlarged, we propose a joint defense system which combines both FSM and SVM for MANETs in this paper.

The rest of the paper is organized as follows. In Section II, let us first examine the vulnerability of AODV and introduce the support vector machine. Then, we describe the proposed joint defense IDS system in Section III. Section IV conducts relevant numerical experiments for the proposed system. Finally, Section V concludes the paper.

II. Vulnerability of AODV and Support Vector Machine

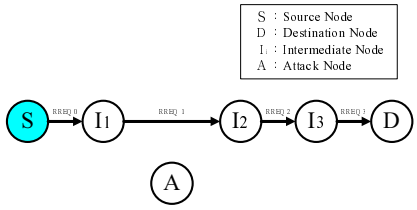
A. Vulnerability of AODV

Before designing our joint defence IDS system, let us first briefly review the vulnerability of AODV. In the literature, the following categories of attacks to AODV have been reported [8], [13], [16]:

- *Authentication Attack*: Authentication in MANETs means the process to authenticate a mobile node to make sure it is a legal node or not. For routing protocols in MANETs, IP and MAC addresses are frequently used to represent identifications of mobile nodes. Hence, to create a fake IP or MAC is the simplest attack of this category, which is usually called *spoofing attack*.
- *Availability Attack*: Availability means to afford network resources, e.g., bandwidth, and services, e.g., connectivity, for legal mobile nodes. Hence, malicious nodes/attackers may interrupt the network through *denial of service* (DoS), including dropping of packets (also unknown as *black hole attack*), *fabrication attack* in which RERR packets are repeatedly sent by a malicious node on a path, *resource consumption attack* in which one or many RREQ packets containing a non-existent destination are broadcasted to cause RREQ flooding, resulting in wastage of bandwidth, *selective existence attack* etc.
- *Integrity Attack*: Integrity stands for no modification to content during transmission. Some possible attacks to AODV of this category include: 1) *false message propagation attack* on the number of sequence number, the number of hops etc., 2) *man-in-the-middle attack* for which an attack/malicious node tries to let it become one node of an existing path. Fig. 1 illustrates steps for the man-in-the-middle attack.
- *Confidentiality and Privacy Attack*: Confidentiality means that the information of a mobile node is only allowed to be accessed by some permitted nodes and privacy means that the information pertinent to a mobile node is not disclosed. This category includes *location disclosure attack* and *content disclosure attack*.

B. Introduction to the Support Vector Machine

SVM is one of branches of machine learning theory and can be applied to solve problems of classification and regression in a reasonable time. It is capable of reducing training and testing errors and has good prediction based on the well-trained model. Taking classification as an example using a linear classifier, SVM tries to find a hyperplane denoted by $f(x) = w \cdot x + b$ based a training data set so that this hyperplane



(a) Source S initiates a path discovery.

(b) Destination D unicasts a RREP to the source and a path $SI_1I_2I_3D$ is established.

(c) Attack node A sends a fake RREQ to I_2 and a fake RREP to I_1.

(d) The path from the source to the destination is changed to $SI_1AI_2I_3D$.

Fig. 1. Steps of the man-in-the-middle attack.

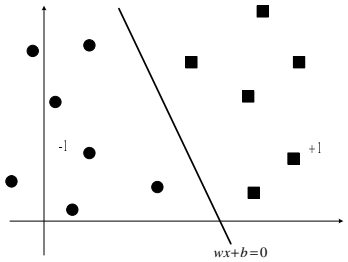


Fig. 2. A hyperplane classifier for SVM.

can separate this data set into two different sets. This idea is illustrated by Fig. 2. Based on values (positives or negatives) of $f(x)$, one is able to classify other new input data. To have lower testing error, an optimal hyperplane with the largest margin between the two separated training data sets can be found as shown in Fig. 3 through *quadratic programming* using Lagrangian and Lagrangian multiplier [14]. Of course, one may not use the linear classifier for most situations. To employ the linear classifier, one needs a non-linear mapping function denoted by Φ to transform the original data set into a feature space so that the linear classifier is applicable (see Fig. 4).

III. Design of the Joint Defense IDS System

Let us now describe our joint defense IDS system for MANETs. This system is based on the AODV routing protocol [10] and can be applied to other routing protocols with a few modifications. Similar to the architecture in [19], we propose

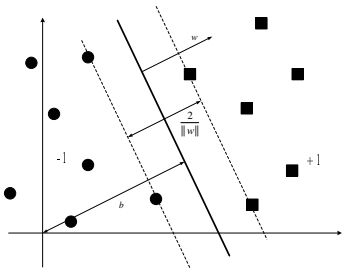


Fig. 3. An optimal hyperplane classifier and the margins.

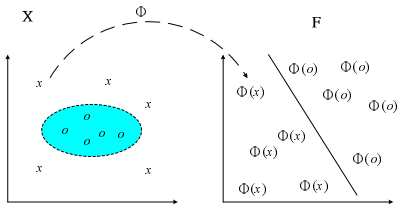


Fig. 4. Data transformation to the feature space through the non-linear mapping.

the architecture for our intrusion detection system combing FSM and SVM as shown in Fig. 5. The reason why we combine FSM and SVM but not two SVMs is that FSM can prevent the system from *zero-day attack* for known attacks before SVM is ready for detection after the well-trained model is formed. For each node with such an IDS, it performs the following functions: data collection, intrusion detection, response, which are described respectively as follows.

A. Mechanism of Data Collection

Through the wireless network card of each mobile node (MN), packet information for an MN can be collected, including information in control packets and information in data packets. Passing the collected information to the detection engine in the mechanism of intrusion detection to be described in the following, we can detect possible attacks.

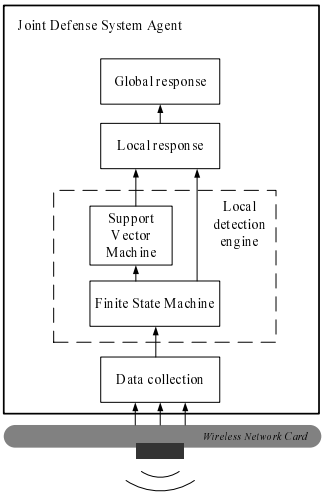


Fig. 5. The proposed joint defense IDS system architecture.

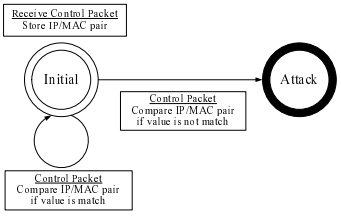


Fig. 6. FSM for the spoofing attack.

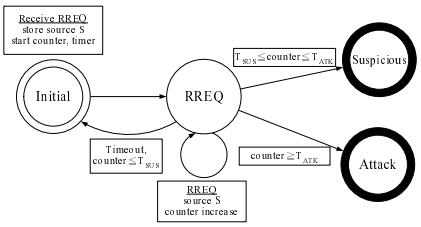


Fig. 7. FSM for the RREQ flooding attack.

B. Mechanism of Intrusion Detection

In the following, we design a mechanism so that less tests are required to make a decision but still maintain the accuracy of detection. To achieve this goal, the FSM strategy is first applied at the first stage. If the FSM strategy is not able to assure the node is a normal node, then the SVM is utilized at the second stage. Defining two values of threshold, i.e., *suspicious threshold* and *attack threshold*, three types of user behavior can be got, i.e.,

- **Normal Behavior:** We are able to say that the user is a *normal* user if the accumulated value is less than the value of suspicious threshold by observing features of packets. Meanwhile, the corresponding feature is generated for use of SVM.
- **Suspicious Behavior:** If the accumulated value is above the value of suspicious threshold but smaller than the value of attack threshold by observing features of packets, we shall not make a definite decision and merely label the behavior as *suspicious behavior*. Then, packets of this suspicious behavior will be checked by SVM at the second stage to make a final decision.
- **Attack Behavior:** If the accumulated value is above the value of attack threshold by observing features of packets, an attack will be recorded. Meanwhile, the corresponding feature is generated for use of SVM.

In the proposed IDS, we design the FSM to specifically detect *spoofing attack*, *RREQ flooding attack*, and *man-in-the-middle attack*. Let us now describe the FSM mechanisms for these attacks. Shown in Fig. 6 is the FSM design for spoofing attacks. It is similar to AODVSTAT in [16]. First, use a table to record the information of IP/MAC. If the stored information of IP/MAC mismatches the information in packets, then the state of FSM will be changed to state of being attacked. Since the determination of mismatch of IP/MAC addresses can be definitely done, the SVM at the second stage is not required. As for RREQ Flooding attack, the design is shown in

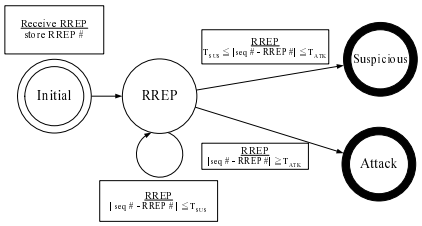


Fig. 8. FSM for the man-in-the-middle attack.

Fig. 7. By employing a counter along with a count-down timer with a pre-specified initial value to count the received number of RREQ packets from a source node, the FSM is able to classified the user behavior based on the number stored in the counter and respond properly. In Fig. 8 the FSM mechanism of man-in-the-middle attacks is shown. To detect this attack, we need to store the sequence number of the RREQ packets and compute the difference of the sequence number of RREQ in of a mobile node and the stored sequence number. Based on the difference, one is able to classify the user behavior.

As for the SVM, we employ SVM^{Light} [6] to train a support vector machine from some features, including time stamps, total number of RREQ packets received for each mobile node, total number of RREQ packets from a source node, difference of RREQ packets between that stored in a table and that in the mobile node as shown in Table I after gathering features for normal and abnormal behaviors marked. More specifically,

TABLE I

PARAMETERS MEASURED FOR A SVM MODEL

Parameter	Description
Time	The time that the feature is generated.
RREQrec[i]	Total RREQ packets that node i has received.
RREQsrc[i][j]	Node i detects the number of RREQ packets that send out by node j.
RREQseqdiff[i][j]	The difference between the sequence number in node i and the sequence number in RREQ packet that send out by node j.

this support vector machine is designed for further analysis on packets with suspicious behavior marked.

C. Mechanism of Responses

Regarding how to take a response to possible attacks, we adopt the following procedure. For the sporadic attacks, we discard the packet without further forwarding it and update the corresponding number stored in a table indicating the number of packets received from the source node (suspicious attacker). Using this table, frequency of attacks from a specific node can be recorded. For some nodes which have high frequencies to send attacking packets (here high frequency means the frequency more than a pre-defined level), we can blacklist them. Afterwards, all packets from nodes in the blacklist are discarded directly or all these nodes are not allowed to join routing tables unless a formal statement to claim the node is a normal node is received. Through distribution/delivery of the blacklist, other nodes in the ad hoc network is able to take a proper response to avoid attacks to the network.

IV. NUMERICAL EXPERIMENTS AND DISCUSSIONS

In this section, we use ns-2 [9] ver. 2.27 along with SVM^{Light} [6] operated in off-line manner to evaluate the proposed IDS. The performance metrics include detection rate and false alarm rate etc. Using models/parameters in Table II, we arrange simulations to evaluate the proposed system. For simplicity, the mechanism of response is just discarding

TABLE II

SETTINGS OF THE SIMULATION ENVIRONMENT

Parameter	Value / Choice
Topology	$1000m \times 1000m$
Simulation time	300 second
Node number	30 or 50
Attack node number	3 or 5
Traffic type	UDP
Packet size	512 bytes
Packet generation rate	4 packets/sec
Node movement model	Random way point model
Node movement speed	5, 10, 15, 20 m/sec
Pause time	2 seconds
Feature sampling interval	3 seconds

packets from malicious nodes. The attack nodes are allowed to perform *IP/MAC spoofing attack*, *RREQ flooding attack*, and *man-in-the-meddle attack*. As for nodes with IDS, they are randomly selected and the ratio of number of nodes with IDS to number of total nodes varies from 20% to 90% with step of 10%. To obtain metrics, we collect 10 observations to have the average value.

A. Results and Discussions

Let us first define the following two metrics

$$\text{Detection Rate (\%)} = \frac{\text{TP}}{\text{TP}+\text{FN}} \times 100\%,$$
$$\text{False Alarm Rate (\%)} = \frac{\text{FP}}{\text{FP}+\text{TN}} \times 100\%,$$

where TP, TN, FP, and FN represent true positive, true negative, false positive, and false negative, respectively, regarding attack detection. From simulations, detection rates of the system can achieve 94%, 90%, 95% for IP/MAC spoofing attack, man-in-the-middle attack, and RREQ flooding attack, respectively, at the first stage (i.e., using FSM solely). With the aid of SVM, detection rates for man-in-the-middle attack and RREQ flooding attack can be further improved to 92% and 99%, respectively. These are shown in Table III. From this

TABLE III

DETECTION RATE AND FALSE ALARM RATE OF ATTACKS

	FSM		FSM+SVM	
Attack type	Detection rate	False alarm rate	Detection rate	False alarm rate
IP/MAC spoofing	94.21%	6.82%	–	–
Man-in-the-middle	89.50%	5.42%	91.63%	7.83%
RREQ flooding	95.41%	6.58%	99.47%	1.25%

table, we also know that different attacks should be solved by different strategies. For example, SVM is not necessary in helping detect IP/MAC spoofing attack. That is why we want to design the joint defense IDS system which employs FSM and SVM to combat attacks. Further comparing with [4], our system can shorten the decision time since FSM needs no

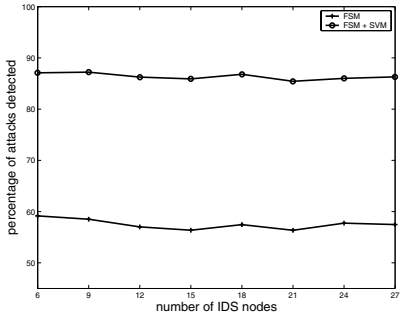


Fig. 9. Detection rate per IDS node (percentage of RREQ flooding attacks detected) vs. number of IDS nodes (the number of total nodes is 30).

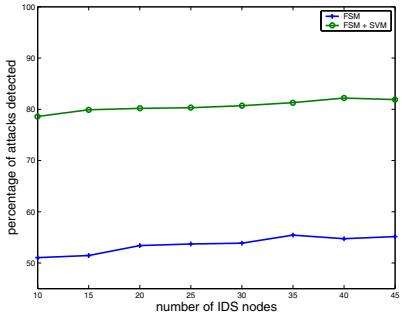


Fig. 10. Detection rate per IDS node (percentage of RREQ flooding attacks detected) vs. number of IDS nodes (the number of total nodes is 50).

training time but 1-SVMDM does. Moreover, our system has a comparable detection rate with the system proposed in [4].

Note that the system overall has a detection rate higher than 95% for RREQ flooding attack using the above-defined metric. But, we now use another way to gauge the detection rate per IDS node. The new detection rate is defined as follows:

$$\text{Detection Rate per IDS Node } (\%) = \frac{D_{ATK}}{T_{ATK} \times T_{IDS}} \times 100\%,$$

where T_{ATK}, T_{IDS}, and D_{ATK} denote the total number of attack nodes, the total number of nodes with IDS, and the total number of attack nodes detected by IDS nodes, respectively. This metric can be interpreted as the percentage of attack nodes detected by an IDS node. Focusing on the RREQ flooding attack, we have results of detection rate per IDS node vs. number of IDS nodes for numbers of total nodes equal to 30 and 50 in Figs. 9 and 10. From Fig. 9 (Fig. 10), we know that about 58% (53%) of attack nodes can be detected by FSM while FSM plus SVM can reach about 86% (80%). The above results further strengthen that the necessary of a joint defence system because only about half of attack nodes are detected although FSM works, while SVM needs more longer decision time but it can detect more malicious nodes.

V. Conclusions

A joint intrusion detection system combing FSM and SVM for MANETs is proposed in this paper. The system not only has a higher overall detection rate, but also shortens the time of decision making. Moreover, it obviously enlarges the detection scope than the single-technique, e.g., FSM, SVM, system.

Acknowledgment

The first author thanks the partial support in finance by the National Science Council, Taiwan under Contracts NSC 93-2219-E-011-007 and NSC 94-2219-E-011-006.

References

[1] Y. Bai and H. Kobayashi, "Intrusion detection systems: technology and development," in *Proc. IEEE AINA '03*, pp. 710–715, Mar. 2003.
[2] S. Bhargava and D. P. Agrawal, "Security enhancements in AODV protocol for wireless ad hoc networks," in *Proc. IEEE VTC '01*, vol. 4, pp. 2143–2147, Oct. 2001.
[3] T. M. Chen and V. Venkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Computing*, pp. 35–41, Nov.–Dec. 2005.
[4] H. Deng, Q. A. Zeng, D. P. Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," in *Proc. IEEE VTC '03*, vol. 3, pp. 2147–2151, Oct. 2003.
[5] A. Hijazi and N. Nasser, "Using mobile agents for intrusion detection in wireless ad hoc networks," in *Proc. IEEE WCNC '05*, 2005.
[6] T. Joachims, SVM^{Light}, http://svmlight.joachims.org/
[7] O. Kachirski and R. Guha, "Intrusion detection using mobile agents in wireless ad hoc networks," in *Proc. IEEE KMN '02*, pp. 153–158, Jul. 2002.
[8] P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad hoc routing protocols," in *Proc. IEEE Information Assurance Workshop* '03, June 2003, pp. 60–67.
[9] The network simulator – ns-2, http://www.isi.edu/nsnam/ns/
[10] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing," in *Proc. IEEE WMCSA '99*, pp. 90–100, Feb. 1999.
[11] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," Internet Draft, draft-ietf-manet-aodv-13.txt, February 2003.
[12] F. Stajano and R. Anderson, "The resurrecting ducking: Security issues for ad-hoc wireless networks," in *Proc. International Workshop on Security Protocols*, 1999.
[13] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV," in *Proc. ACM SASN '03*, pp.125–134, 2003.
[14] V. Vapnik, "The nature of statistical learning theory. springer," 1995.
[15] L. Venkatraman and D. P. Agrawal, "A security scheme for routingin ad hoc networks," in *Proc. IEEE WCNC* '00, 2000, pp. 1268–1273.
[16] G. Vigna, S. Gwalani, K. Srinivasan, E. M. Belding-Royer, and R. A. Kemmerer, "An intrusion detection tool for AODV-based ad hoc wireless networks," in *Porc. IEEE ACSAC '04*, pp. 16–27, Dec. 2004.
[17] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proc. ACM MobiHoc '01*, pp. 299–302, Oct. 2001.
[18] M. G. Zapata and N. Asokan, "Securing ad-hoc routing protocols," in *Proc. ACM WiSE '02*, pp. 1–10, Sep. 2002.
[19] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in *Proc. ACM MobiCom '00*, pp. 275–83, Aug. 2000.
[20] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," in *Proc. ACM WINET '03*, vol. 9, no. 5, pp. 545–556, Sep. 2003.