Dynamic Distributed Authentication Scheme for Wireless LAN-Based Mesh Networks

Insun Lee[1], Jihoon Lee[1], William Arbaugh[2], and Daeyoung Kim[3]

[1] Comm.& Conncetivity Lab., Samsung Advanced Institute of Technology
P.O. Box 111, Suwon, 449-716, Korea
{insun,vincent.lee}@samsung.com
[2] University of Maryland, USA
waa@cs.umd.edu
[3] Information and Comminications University, Korea
kimd@icu.ac.kr

Abstract. Wireless LAN systems have been deployed for wireless internet services for hot spots, home, or offices. Recently, WLAN-Based Mesh Networking is developed with the benefit of easy deployment and easy configuration. Due to the characteristic of distributed environment, Wireless Mesh Networks(WMNs) need a new authentication scheme which allows multi-hop communication. In this paper, we propose a distributed authentication method which significantly eases the management burden and reduces the storage space on mesh points, thus enables the secure and easy deployment of WMNs.

Keywords: Wireless Mesh network, Distributed authentication, WLAN.

1 Introduction

Traditional single-hop network architecture dominates the current wireless and mobile communication technology. However, it imposes several limitations on its deployment in terms of coverage, cost, capacity and scalability. For example, widely deployed IEEE 802.11-based wireless LANs require a wired connection on each dedicated access point (AP). Since all mobile stations (STAs) need to be connected to a single AP, network throughput becomes poor with many stations operating simultaneously. Alternatively, multi-hop communication is known to overcome these limitations of single hop networking. Until recently, multi-hop techniques had been studied only in context of mobile ad hoc networks (MANETs).

Similar to MANETs, Wireless Mesh Networks (WMNs) is emerging as a multi-hop mobile network. Wireless mesh allows many individual nodes to be interconnected automatically with computers nearby, to create a large-scale, self-organizing network. Mesh is increasingly being adopted as an alternative to cable or DSL which are used for last-mile coverage[3]. In wireless mesh networks, intermediate nodes can function as a router to forward data transmitted from the source to a destination that is located in more than one hop away.

T. Vazão, M.M. Freire, and I. Chong (Eds.): ICOIN 2007, LNCS 5200, pp. 649–658, 2008.

Following list shows potential strengths of WMNs:

- Self-configuration: Mesh networks are self-organizing and self-configuring in the sense that they relieve service providers and/or IT departments from continuous administration. Deployment of mesh network also becomes easy and fast compared to other types of networks.
- Increased reliability: Redundant links in mesh networks provides added reliability even if some nodes fail to function.
- Increased capacity: Use of multiple channels and interfaces provides extra spatial reuse of available bandwidth, and it enables multiple data flows co-exist in the shared medium, thus the overall network capacity is increased.
- Coverage extension: Mesh network's multi-hop communication enables covering dead-zones. Any reachable mesh node can relay the traffic, so connectivity and network access can be provided.
- Energy conservation: Multi-hop communication, smart routing and medium access co-ordination contribute for saving power for energy-constraint devices.

In spite of its useful functions and characteristics, WMNs lack of efficient and scalable security solutions, because their security can more easily be compromised due to several factors: their distributed network architecture, the vulnerability of channels and nodes in the shared wireless medium, and the dynamic change of network topology [1]. Attacks on routing protocols and Medium Access Control(MAC) protocols are possible. For example, the backoff procedures and NAV for virtual carrier sense of IEEE 802.11 MAC may be misused by some attacking nodes, which causes the network to always be congested by these malicious nodes. WMNs wireless link is vulnerable to attack like other wireless medium, so a cryptographic protection has to be provided.

IEEE 802.11i standard[12] defines the security architectures for protecting the link layer between two entities- STA and AP. It provides the security architecture such as authentication, confidentiality, key management, data origin authenticity and replay protection. Authentication framework of this standard is for both infrastructure mode ad-hoc mode(IBSS mode). This authentication framework uses a combination of several protocols such as IEEE 802.1X and transport layer security(TLS). As shown in Fig.1, authentication is performed through the interaction of three entities- STA, AP, and Authentication server.

Authentication is performed to make only legitimate nodes can access the network. For infrastructure WLAN, this is performed through a centralized server such as RADIUS (Remote Authentication Dial-in User Service). Such a centralized scheme is not suitable for WMNs, where the network topologies are dynamic and distributed due to mobility and network failure that comes from their ad-hoc feature. Moreover, key management in WMNs is much more difficult than in infrastructure wireless LANs, because it's more complicated for a central authority to handle the distributed network, and the dynamic characteristic of WMNs makes the key management more complicated. Key management in WMNs needs to be performed in a distributed but secure manner. Therefore, a distributed authentication and authorization scheme with secure key management is needed for WMNs. Distributed Authentication with a public key infrastructure is straight forward for the implementers. It is, however, a major management and operational hurdle for end users. Historically, PKI's have only been

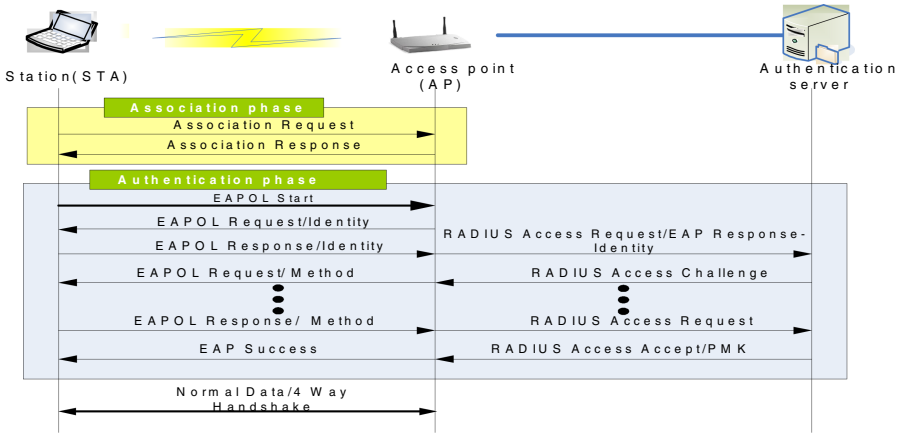

Fig. 1. IEEE802.11i Authentication model based on IEEE802.1X

attempted by large well-funded organizations and not by smaller organizations and home users. Yet these people (the SoHo users) are the very end users a distributed authentication mechanism is meant to target.

In this paper, we propose a novel distributed authentication algorithm which is suitable for WMNs. In our approach, the administrator does not have to provide each mesh point with the keys of all other mesh nodes, and a key for the authenticating station need only exist some where within the mesh. This significantly eases the management burden and reduces the storage space on mesh points.

The rest of the paper is organized as follows. Section 2 briefly describes some related works in WLAN and mesh networks. Section 3 presents the design and detailed description of Dynamic Distributed Authentication(DDA) scheme. Then, we present the evaluation results of analytical modeling and then finally we made a conclusion.

2 Related Works

Security issues on wireless mesh networks are very similar to those in sensor or ad-hoc networks, and these were well evaluated on the previous literatures[11]. Because of their large scale and dynamic topology change, key establishment based on public-key or symmetric key is one of the issues in wireless ad-hoc networks. Chan[9] and Jolly[8] introduced efficient key distribution schemes which have benefit for low power sensor nodes. TinySec[7] provides link layer encryption mechanism for access control, integrity, and confidentiality for TinyOS. This mechanism uses a symmetric key scheme for link layer data protection. TESLA[11] introduces an authenticated broadcast scheme which uses purely symmetric primitives and introduce asymmetry with delayed key distribution.

But these security problems and their solutions are not directly applicable to WMNs. The most important fact that impacts the performance for ad hoc sensor networks is power consumption, so important parameter that affects the performance of the security function is power consumption. The above schemes were designed for

ad-hoc sensor networks where thousands of nodes are distributed over the large area, and the proposed schemes were based on the centralized access control under the assumption of existence of the central authority.

On the other hand, usage models for WLAN based WMNs includes office, residential, campus, public, safety/military networks[14]. As well as the power consumption, easier installation is one of the most important functionality that is necessary for rapid deployment of WMNs. Most of the proposed security schemes for ad-hoc network assume that every node has pre-shared secret before the installation, and authentication is performed by using this pre-shared secret. But pre-installing of the shared secret of every node is a critical overhead for the network consisting of large number of entities.

Authentication in IBSS mode is defined in 802.11i for ad-hoc communication, where one hop peer-to-peer communication is performed. This is a candidate authentication method for WMNs. But, to use this with either certificate or pre-shared key(PSK), all the certificates or keys of the nodes have to be pre-installed in each node. Also, authentication has to be performed twice between two nodes. i.e. one node plays the role of authenticator and supplicant in each authentication. Thus when there are N nodes in a WMN, N*(N-1) number of keys have to be maintained for the WMN, which results in high key management overhead. Thus an efficient authentication method for mesh needs to be provided.

3 Dynamic Distributed Authentication (DDA) Scheme

This section describes the detailed design of DDA scheme. First, we show the background and architecture of the proposed scheme. After that, we explain DDA scheme that performs the dynamic distributed authentication in detail.

3.1 Overview

As shown in the previous chapters, authentication and key management is one of the important hurdles for the deployment of Wireless Distributed Systems(WDS) which construct WMNs. In this section we introduce a novel distributed authentication mechanism that offers a high scalability. Especially, this algorithm allows small enterprises to use a shared secret mechanism and still allows a multi-hop environment to grow beyond a single AP in WDS. This method can enable the installation of the WDS easier, thus it enhance the easy deployment of WDS.

If an organization were to use the existing IBSS authentication for the Mesh, then the administrator would have to provide every mesh point with the key for every station. In a dynamic organization, this management burden would be intolerable. The only solution, currently, is to install a AAA server and perform centralized authentication. But, this management burden may be too heavy as well.

In our approach, the administrator need only establish a PSK with only one mesh point within the WMN and the station. The protocol, described below, will automatically find a shared key in the WMN if it exists, and establish a new fresh secret between the station and the mesh point to which this station is associating.

The typical usage scenario for this method will be that a small enterprise purchases a single AP to support one or more STAs. The usual form of security in this scenario will be to establish a shared secret between the AP and the STAs. This works without the need for a AAA server. But, it cannot grow easily beyond the single AP scenario without tedious manual key management. This algorithm is designed to allow the enterprise to add APs easily and still provide the same degree of security as the single AP case without additional work for the administrator.

A second scenario that this algorithm supports is when two isolated WDS join to form a single WMN. The system administrator need only establish a single shared secret between the two connecting APs, then STAs from each WDS will be able to roam freely between the two systems.

Our approach combines a modified Otway-Reese protocol with broadcasting for a novel distributed authentication algorithm within dynamic topologies that easily integrates into the extensible authentication protocol (EAP) and the IEEE 802.11i protocol. Otway-Reese Protocol is a proven security protocol for authentication and key exchange between 3 parties[10]. Our protocol uses the reactive routing protocol which is a mandatory routing protocol of IEEE802.11s standard which defines the WLAN based Mesh Networks.

Our notion is that all entities within a WDS are first class principals. That is both an AP and a STA authenticate in exactly the same method, i.e. both contain an IEEE 802.1X supplicant and authenticator module. In the rest of this paper, we identify the principals in an authentication as the STA for the MP(Mesh Point) that wants to join the WDS, and AP for the MP or Mesh Access Points. If a new AP wishes to join the WDS, then that AP acts as STA for the purposes of this protocol.

3.2 Operation Procedures of the Proposed Scheme

There are two cases we need to consider for authentication in WDS. The first is when the STA wishes to associate with an AP with which it shares a security association which may be either a shared secret or a public key certificate derived from a common authority, or the AP communicates directly with a central AAA server. The second is when the STA wishes to associate with an AP with which it doesn't share a secret, i.e. the AP can not authenticate the station directly nor through a AAA server. In the first case, the standard 802.11i protocol and EAP can be used. In the second case, our algorithm is used in conjunction with the 802.11i protocol to make the authentication of the STA possible in distributed manner.

Our approach enables the authentication without a common security association. When a STA wishes to associate with an AP, with which it does not share a secret, the AP will broadcast the identity of the STA to the WDS in the hopes of identifying an AP within the WDS with which the STA does share a secret. If no AP is found, then the STA cannot be authenticated. If an AP is found, then there are two cases. The first is when the Trusted AP (T) is one hop away from the requesting AP (i.e. T is a neighbor of the requesting AP), and the second is when the T is more than one hop away from the requesting AP. In both cases, reactive routing protocol is used to find T as described in the following section. Fig. 2 depicts the multi hop case.

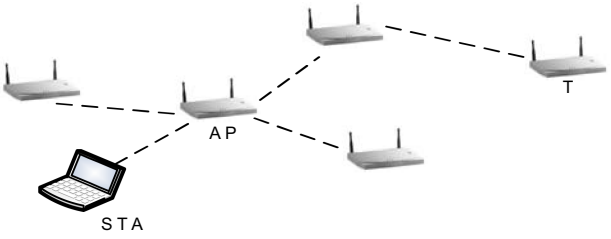

Fig. 2. Multi hop authentication

The protocol uses the following terminologies and has the following assumption for the compatibility with the current 802.11i;

Terminology	Description
E	Encryption E is AES-CCM that is the mandatory encryption method for 802.11i
$E_{K_{A\leftrightarrow B}}(C)$	Means that C is encrypted with AES-CCM with the secret key between A and B
K	128 bit session key that T generates for STA and AP to share
N_{STA}, N_{AP}, N_T	256 bit nonces chosen by STA, AP, and T respectively
M	256 bit transaction identifier chosen by STA

The authentication protocol is as follows. It consists of four phases :

i. Initializing the authentication
ii. Finding T(i.e. finding the Trusted AP)
iii. Authentication and key distribution
iv. Session key distribution

The detailed operation procedure of the proposed scheme is as follows:

Phase 1: Initializing the authentication
As shown in Fig.3, STA starts Traditional EAP to start the authentication procedure. On receiving EAP-START message from STA, AP request the STA's identity,then STA sends its identity to AP. This makes our method compatible with 802.11i.

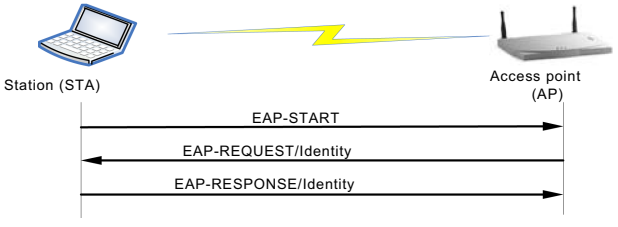

Fig. 3. Initialization of authentication

Phase 2 : Finding T .
In this phase, AP needs to find T. When the STA send the EAP-Response/Identity message to AP in Phase1, STA may or may not know the identity of T. If it knows the identity of T, it can send AP the identity of T. On receiving the identity of T, AP need to check the MeshID of T. Then there are two cases- The Mesh ID of T is the same as that of AP or not.

When the Mesh ID of T is the same as that of AP, AP will check its routing table to check if T is in its routing table. If T is in its routing table, then phase 2 is over. If T is not its routing table, then it sends the "T lookup request message" with the action frame in the RREQ message of IEEE802.11. On receiving this RREQ message, T sends RREP message to AP, and now the route between AP and T is established. If the Mesh ID of T is not the same as that of AP's, T and AP are not in the same WDS. In this case, sending RREQ message and RREP massage procedure is the same, but we should follow the interworking protocol that is used in the given mesh network.

If the STA doesn't know the identity of T, then on receiving EAP-Response/identity message from the STA, AP broadcast the "T lookup request message" using the action frame of the RREQ in the hope of finding T. In this case, AP sends STA's Identity in the action frame to ask the WDS if any node knows this STA. When T, who has pre-shared secret with STA, receives this RREQ, it'll send the RREP message to AP with the routing information. If more than one T responds to the requesting AP, then AP may use any algorithm such as thresh-hold scheme to select one T.

On receiving the RREP, the requesting AP will pick a T with which it already shares a secret. If the requesting AP does not share a secret with any of the responding T, then the closest responder is selected and a shared secret between AP and this responder has to be established prior to responding to the STA. For this, our algorithm works for the requesting AP, and this requesting AP plays the role of the STA of our algorithm at this time.

Using our algorithm, each node in WDS only need to maintain the keys which are authenticated to it, so the number of keys that is to be maintain for each nodes are the number of nodes that are authenticated to that nodes.

Phase 3: Authentication and Key Distribution
In this phase, modified Otway-Reese Protocol is used to distribute the key, k, between AP and STA. Through this step, AP and STA perform the mutual authentication, and share k at the end of the authentication phase.

T, which was found as the result of phase 2, sends nonce N_T to AP for generating k. N_T is encrypted with the key $K_{T\leftrightarrow AP}$ and $K_{T\leftrightarrow STA}$ for AP and STA respectively. On receiving this nonce from T, AP relays N_T which is encrypted with $K_{T\leftrightarrow STA}$ to STA. Now STA received N_T and it generates its nonce N_{STA} and encrypts N_{STA} and N_T with $K_{T\leftrightarrow STA}$. At this time STA may generate the transaction ID, M, for anonymity purpose. Then STA sends this packet with its ID to AP and AP relays this packet to T. By doing this, STA can show its authenticity to T. At the time AP relaying this packet to T, AP also generates its nonce N_{AP} and sends it to T encrypted with the key $K_{T\leftrightarrow AP}$, so that AP can show its authenticity to T. On receiving both N_{STA} and N_{AP}, T can

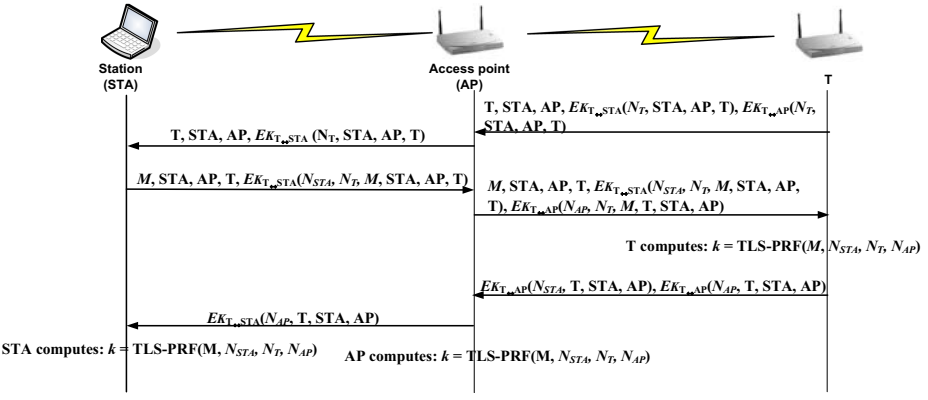

Fig. 4. Authentication & Key distribution phase

compute the master key k using the TLS-Pseudo Random function (TLS-PRF). Then T sends N_{STA} and N_{AP} to AP and then AP relays N_{AP} which is encrypted with $K_{T\leftrightarrow STA}$. Now both AP and STA have N_T, N_{AP}, and N_{STA} so that they can generate the master key k. Now authentication and key distribution is accomplished. Fig. 4 summarizes this procedure.

Phase 4: The last phase is for achieving the session key. This ensures that only the AP and STA know the derived session key as well as proving freshness. Following the completion of the above protocol, AP and STA can complete the IEEE 802.11i 4-way handshake for compatibility with the standards.

In summary, DDA scheme eases the key management burden of WMNs. Also, it reduces the control message overhead induced by single point failure problem by using the distributed authentication scheme.

4 Analytic Evaluation

In this section, we analyze how much our scheme reduces the expected authentication latency. In our simulation, we used the NS-2 implementation of the IEEE 802.11b physical layer and MAC protocols. The radio model was modified to have a nominal bit rate of 11Mb/sec while supporting a transmission range of 250 meter. In addition, we chose as a routing protocol model the Ad Hoc On-demand Distance Vector (AODV) protocol [6]. A peer relationship can be established when two nodes are located in close proximity. We use the random walk mobility model with various pause times and maximum speed [13].

Fig. 5 shows that the authentication delay increases when the load over the network increases regardless of the authentication type (i.e., existing scheme or proposed scheme). However, the proposed scheme has lower authentication delay compared to the existing scheme with the centralized architecture because of the distribution of authentication traffic.

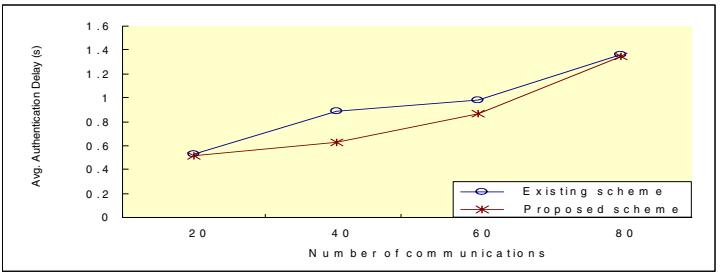

Fig. 5. Effect of distributed authentication in terms of authentication delay

Generally, the objective of increasing the number of node with the authentication functionality is to distribute the load over the nodes, hence, to enhance the performance of the authentication operation and the performance of the network accordingly.

Our simulation (Fig. 6) shows that as the number of trusted nodes (T) is increased, the authentication delay is decreased for multiple communications. This is expected since the distribution of authentication nodes should reduce the authentication overhead, which is expected to positively affect the performance of the authentication operation and hence the network performance. Note that the backoff effect of authentication is decreased by increasing the number of authentication nodes. Therefore, while the increase of the number of authentication nodes tend to decrease the authentication delay due to load distribution, the load on the network increases as a result of having faster flow start. Consequently, this leads to more packets in the network, which may lead to increasing the authentication delay due to contention/interference characteristics of IEEE 802.11 interface.

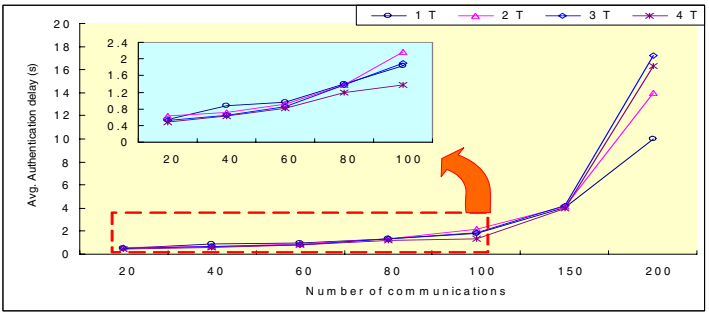

Fig. 6. Authentication delay as the number of communications increases for variable authenticator nodes

5 Conclusion

In this paper, we proposed a Dynamic Distributed Authentication (DDA) method for WMN. Instead of using a central authentication server, we distributed the trusted nodes (T) which can play the role of authentication server over the WMN. This

enables the authentication of the new STA possible even though it doesn't have pre-shared key with the immediate neighbor AP or AP doesn't directly communicate with the central AAA server. Thus the authentication and key management of the network becomes simpler, and the end users can easily develop the Wireless Mesh Network using WLANs. We showed that authentication delay is decreased as the number of the trusted node (T) increases, thus the complexity of the network overhead is also decreased, and the network management is also efficient.

References

1. Akyildiz, I.F., Wang, X.: A Survey on Wireless Mesh Networks. IEEE Radio Comm. Mag., 23–30 (September 2005)
2. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications 11(1), 38–47 (2004)
3. Perkins, C., Belding-Royer, E.: Ad-hoc on demand distance vector (AODV) routing. In: IEEE workshop in Mobile computing Systems and Applications (February 1999)
4. Buttyan, L., Hubaux, J.-P.: Report on a working session on security in wireless ad hoc networks. ACM Mobile Computing and Communications Review 7(1), 74–94 (2002)
5. Gong, L.: Increasing Availability and Security of an Authentication Service. IEEE Journal on Selected Areas in Communications 11(5) (June 1993)
6. Pabst, R., et al.: Relay-based deployment concepts for wireless and mobile broadband radio. IEEE Communications Magazine 42(9), 80–89 (2004)
7. Karof, C., Sastry, N., Wagner, D.: TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. In: Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004) (November 2004)
8. Jolly, G., Kuscu, M.C., Kokate, P., Younis, M.: A Low-Energy Key Management Protocol for Wireless Sensor Networks. In: IEEE Symposium on Computers and Communications (2003)
9. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proceedings of Security and Privacy, 2003, pp. 197–213 (2003)
10. Menezes, A., et al.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
11. Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar, J.D.: SPINS: Security Protocols for Sensor Networks. In: Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001 (2001)
12. IEEE Std. 802.11i, IEEE Standard for Telecommunications and Information Exchange between Systems-lan/man Specific Requirements, Part 11: Wireless Medium Access Control and Physical Layer (phy) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements (2004)
13. Capkin, S., Hubaux, J.P., Buttyan, L.: Mobility Helps Security in Ad hoc Networks. In: ACM MobiHoc (2003)
14. IEEE 802.11 TGs document IEEE P.802.11-04/662r14, `http://www.ieee802.org/11`