**Int. J. Communications, Network and System Sciences, 2014, 7, 365-372**
Published Online September 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.79038

# Security Approaches in IEEE 802.11 MANET

## —Performance Evaluation of USM and RAS

**Arif Sari**

Department of Management Information Systems, School of Applied Sciences, European University of Lefke, Lefke, Cyprus
Email: asari@eul.edu.tr

Received 20 January 2014; revised 20 February 2014; accepted 20 March 2014



## Abstract

**Evaluation of IEEE 802.11 Mobile Ad Hoc Networks (MANET) security issues becomes significant concern for researchers since Denial of Service (DoS) attacks are recognized as one of the most harmful threats. A variety of security mechanisms are proposed to solve security dilemma in MANETs against different layers of DoS attacks. Physical Layer jamming attacks exhaust the victim's network resources such as bandwidth, computing power, battery, etc. Unified Security Mechanism (USM) and Rate Adaptation Scheme (RAS) are two of the proposed methods by researchers against DoS attacks. USM and RAS mechanisms are simulated through OPNET simulator and Jamming Attack is generated on the network for each security mechanisms to compare specific performance metrics on the network.**

## Keywords

**MANET, RAS, USM, Denial of Service, Security, IEEE 802.11, Jamming Attack**

## 1. Introduction

Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. A Jamming attacks exhausts the victim's network resources such as bandwidth, computing power, battery etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. DoS defence methods have been proposed since long time, but most of them remain theoretical with no actual implementation or could not produce satisfied results and performance when applied on MANETs. Many of these methods need to be implemented simultaneously and collaboratively on several nodes, making them difficult to implement especially on nodes which are distributed and need to maintain round-the-clock Internet connectivity. Researchers contributed to MANET security field by proposing different approaches to security issues of different network layers. USM is one of the methods proposed by researchers to

**How to cite this paper:** Sari, A. (2014) Security Approaches in IEEE 802.11 MANET. *Int. J. Communications, Network and System Sciences*, **7**, 365-372. http://dx.doi.org/10.4236/ijcns.2014.79038

enhance security and prevent Denial of Service (DoS) attacks through an intermediate strategy by participating modified guard node [1]. A mechanism called RAS have proposed by researchers for detection of jamming attacks through measuring Packet Delivery Ration (PDR) with Signal Strength (SS). Researchers [2], have proposed a solution called "Rate Adaptation Scheme" for detection of jamming attacks through measuring Packet Delivery Ratio (PDR) with Signal Strength (SS). These two mechanisms, USM and RAS are designed to prevent DoS attacks, which is quite serious threat that collapses all necessary components of the system that provides operability and availability of network resources [3]. DoS attacks lead service violations where it causes overhead problem on the network and it requires specific detection and mitigation techniques [4].

## 2. Literature Survey

Denial of service attacks rely on making a server computer's resources unavailable for users by sending huge packages and requests from attacker computers. Attacks are classified by researchers as Jamming, Scrambling and Water Torture [5].

Jamming can be described as an attack "achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel". Jamming can be either intentional or unintentional. It is not difficult to perform a jamming attack because necessary information and equipments are easy to acquire and there is even a book by Poisel which teaches jamming techniques. We can prevent jamming attack by increasing the power of signals or by increasing the bandwidth of signals using spreading techniques such as frequency spread spectrum (FHSS) or direct sequence spread spectrum (DSS) [5].

Scrambling is a kind of jamming but only provoked for short intervals of time and targeted to specific WiMAX frames or parts of frames at the PHY layer. Attackers can selectively scramble control or management information in order to affect the normal operation of the network. Slots of data traffic belonging to the targeted SSs can be scrambled selectively, forcing them to retransmit. It is more difficult to perform a scrambling attack than to perform a jamming attack due to "the need, by the attacker, to interpret control information and to send noise during specific intervals. Since scrambling is intermittent, it is more difficult to detect scrambling than jamming. Fortunately, we can use anomalies monitoring beyond performance norm (or criteria) to detect scrambling and scramblers. This is also a typical attack in which an attacker forces a SS to drain its battery or consume computing resources by sending a series of bogus frames. This kind of attack is considered even more destructive than a typical Denial-of-Service (DoS) attack since the SS which is a usually portable device is likely to have limited resources. To prevent this kind of attack, a sophisticated mechanism is necessary to discard bogus frames, thus avoiding running out of battery or computational resources [5] [6].

Some of the security schemes have been proposed that detection of malicious node depending on node behaviors of the corresponding nodes that are exhibiting malicious behaviors such as packet dropping, packet modification, and packet misrouting and indicated a new proposed solution as a collaborative and trust based outlier detection algorithm that factors in a node's reputation for MANET [7]. Researchers have proposed malicious nodes through path selection technique since the most of the existing security mechanisms in order to detect the packet droppers in a MANET environment generally detect the adversarial nodes performing the packet drop individually wherein false accusations upon an honest node by an adversarial node are also possible [8].

Another novel detection technique has been proposed in the literature which is based on triangular encryption technique. In this technique, agenst are fired from a node for each node randomly and detect the defective nodes. This scheme is an "Agent" based intrustion detection system [9].

In multi hop wireless systems, such as ad hoc and sensor networks, mobile ad hoc network applications are deployed, security emerges as a central requirement. Since DoS attacks are active attacks and it's one of the most dangerous attacks which is difficult to detect and mitigate, researchers conducted a study to detect active attacks in MANET environment [10].

Another broad range of comparative study conducted by researchers in the literature by conducting vulnerability analysis of network layer protocols to identify unsolved threats to the security algorithms, such as, blacks holes, wormholes, Modification, Sybil and rushing attacks. All these vulnerability analysis are compared with security schemes and overall evaluation of proposed schemes simulated to battle the identified threats [11].

## 3. Proposed Mechanism

### 3.1. Unified Security Mechanism (USM)

USM has proposed by the researcher in order to prevent constant jamming attacks through implementing a spe-

cific security mechanism on randomly selected nodes on the network. The proposed method is combination of two mechanisms implemented on Data Link Layer of the mobile nodes. Mechanisms implemented on Data link layer are Point Coordination Function (PCF) and Request to Sent/Clear to Sent (RTS/CTS) mechanisms. An IEEE 802.11 MAC protocol coordinates the transmission of the nodes on the common transmission medium through contention free and contention based polling mechanisms. Researcher has used PCF which is contention free mechanism as shown in the **Figure 1**.

RTS/CTS mechanism is a handshaking process that proposed to minimize collision problem on the network [12]. As it is proposed by researcher, RTS mechanism is implemented with CTS mechanism since the network throughput may degrade due to the Request to Send (RTS) collision problem. Researcher has combined these two mechanisms into a randomly selected mobile node to provide security. The combination of the mechanism is illustrated in **Figure 2**. Due to this combination, the name of the proposed method is called Unified Security Mechanism.

Point Coordination Function (PCF) of the guard nodes are modified at the MAC layer according to the proposed model. This technique is used to coordinate the communication within the network. The PCF mechanism uses base station to control all activities in the network. Base station polls the other station asking them if they have any frame to send. In PCF, as it is centralized, no collision will occur. In addition to this, RTS/CTS mechanism has implemented to recover any potential unauthorized access to the shared medium.

## 3.2. Rate Adaptation Scheme (RAS)

Rate Adaptation Scheme has proposed by the researcher for detection of jamming attacks through measuring

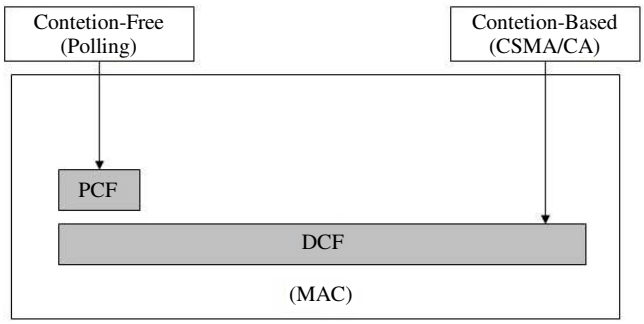


**Figure 1.** 802.11 MAC layer control mechanisms.

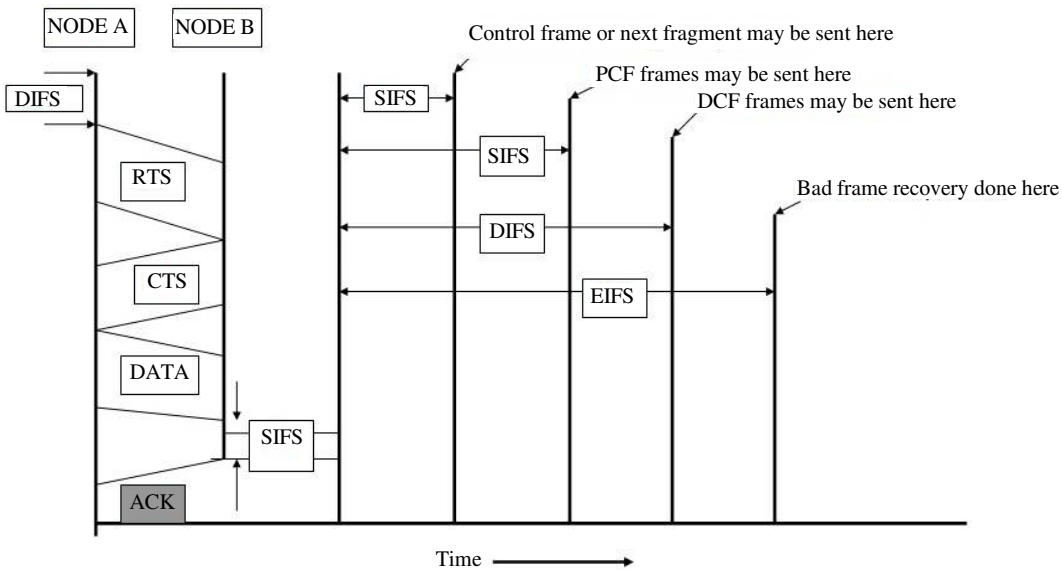


**Figure 2.** Structure of unified security mechanism.

Packet Delivery Ratio (PDR) with Signal Strength (SS) [2]. When a node detects jamming attack, it uses the proposed rate adaptation scheme for data transmission. However the solution relays on the high rate of signal strength while the packet delivery ratio should be low. The proposed jamming attack detection scheme have decided that the channel is jammed if the measured SS value is higher than the signal strength threshold and PDR values are lower than PDR threshold. The thresholds are decided by another researcher's experiment [13]. Researchers have modified Distributed Control Function (DCF) from the Data Link Layer as shown in the **Figure 1** to implement proposed rate adaptation scheme. This scheme has represented through mathematical equation on Equation (1):

$$G^m = \frac{L_{\text{Data}}}{T^m_{\text{Data}}} x \rho^m_s \tag{1}$$

and for successful transmission probability for $\rho^m_s$

$$\rho^m_s = \left(1 - p^m_e\left(L_{\text{Data}}\right)\right)\left(1 - p^m_e\left(L_{\text{ACK}}\right)\right) \tag{2}$$

and approximate successful transmission probability shown in Equation (3),

$$\rho^m_s \approx \left(1 - p^m_e\left(L_{\text{Data}}\right)\right) \tag{3}$$

and in order to calculate the error probability for a data frame, the Physical Layer Convergence Procedure (PLCP), $p^m_e\left(L_{\text{PLCP}}\right)$, and error probability of Mac Protocol Data Unit (MPDU), $p^m_e\left(L_{\text{MPDU}}\right)$ is used to calculate error probability of data frame $\rho^m_s\left(L_{\text{Data}}\right)$ as shown on the Equation (4) below.

$$\rho^m_s\left(L_{\text{Data}}\right) = 1 - \left[\left(1 - p^m_e\left(L_{\text{PLCP}}\right)\right)\left(1 - p^m_e\left(L_{\text{MPDU}}\right)\right)\right] \tag{4}$$

## 4. Simulation Model of Proposed Mechanism

In this section, implementation of proposed models for performance evaluation is described. Simulation scenarios have been designed using OPNET Modeler 14.5 [14]. There are variety of simulators available however the OPNET modeler is one of the most powerful and accurate simulators for simulating MANET environments [15]. The USM has implemented proposed mechanism by modifying 802.11 PCF scheme in OPNET modeler while RAS has implemented proposed mechanism through modifying DCF in data link layer. The simulation parameters are summarized in **Table 1**.

In a network topology, Ad Hoc On-Demand Distance Vector Protocol (AODV) is used as a MANET communication protocol. AODV is one of the reactive protocols. In this protocol when a node wishes to start transmission with another node in the network to which it has no route; AODV protocol provides topology information for the node. In deployment model, total of 50 mobile nodes are randomly distributed in a 1000 × 1000 meters field. In addition to this two mobile jammers are included into scenario to launch constant jamming attack on the network. Nodes move around based on random waypoint mobility model which the node speeds 10 m/s. **Figure 3** shows proposed scenario topology created in OPNET. On the other hand, the specific MANET traffic parameters are set for this simulation experiment.

### 4.1. Traffic Model

The traffic model is used to generate traffic on the network and which a set of applications that generates the packet both exponential and constant form when the simulation time starts with random destination or defined destination packet delivery. Furthermore, it is essential to specify a trajectory for mobile nodes to provide mobility where nodes in the network are constantly moving. **Table 2** shows the MANET Traffic Model parameters.

### 4.2. Performance Metrics

The performance metrics chosen for the evaluation and prevention of jamming attack methods on MANETs are Network Throughput and WLAN Delay. **Table 3**, illustrates the selected performance metrics.

## 5. Performance Evaluation and Comparison of Proposed Mechanisms

In this section, evaluation of USM and RAS is compared in terms of end-to-end MAC delay and average

**Table 1.** Simulation parameters.

| Global Simulation Parameters for the Experiment | |
|---|---|
| Parameters | Attributes |
| Protocol | AODV |
| Simulation Time | 1 hour (60 minutes) |
| Simulation Area | 1000 × 1000 meters |
| Mobility Model | Random Waypoint |
| Mobility meters/seconds | 10 meters/seconds |
| Performance Parameters | Throughput, WLAN Delay |
| Transmission Power (W) | 0.005 W |
| Transmission Range | 2 km |
| RTS Threshold | 1024 |
| Data Rate | Auto Configured |

**Table 2.** MANET traffic model parameters.

| Attribute | Value |
|---|---|
| Trajectory | VECTOR |
| AD-HOC Routing Parameters | |
| Ad Hoc Routing Protocol | AODV |
| MANET Traffic Generation Parameters | |
| Start Time | 10 seconds |
| Packet Interarrival time | 0.03 seconds (exponential) |
| Packet Size (bits) | 2000 (exponential) |
| Destination IP Address | Random |
| Stop Time | End of Simulation |
| WLAN Parameters | |
| Data Rate (bps) | 11 Mbps |
| Channel Settings | Auto Assigned |
| Transmit Power | 0.005 Watt |
| RTS Threshold | 1024 bytes |
| Buffer size | 1,024,000 bits |

**Table 3.** MANET traffic model parameters.

| Performance Metrics |
|---|
| Network Throughput |
| MANET Delay |

throughput. The outcomes of the performance metrics are compared below. According to these parameters, 50 mobile nodes which are already used in this research have simulated to compare the proposed techniques. The results of the comparison illustrated in **Figure 4** and **Figure 5**.

As it is shown on **Figure 4**, the proposed mechanism by researcher is compared in terms of average throughput. The throughput represents the total number of bits (in bits/seconds) forwarded from Wireless LAN layers to higher layers in all WLAN nodes of the network. The duration of the simulation was 300 seconds while number of seeds used 300 to provide 1 hour simulation performance. Based on this outcome, **Figure 4** clearly states that, the performance of USM has shown better performance in terms of throughput. **Figure 5** illustrates the comparison of USM and RAS in terms of WLAN Delay. The WLAN Delay represents the end-to-end delay of all packets

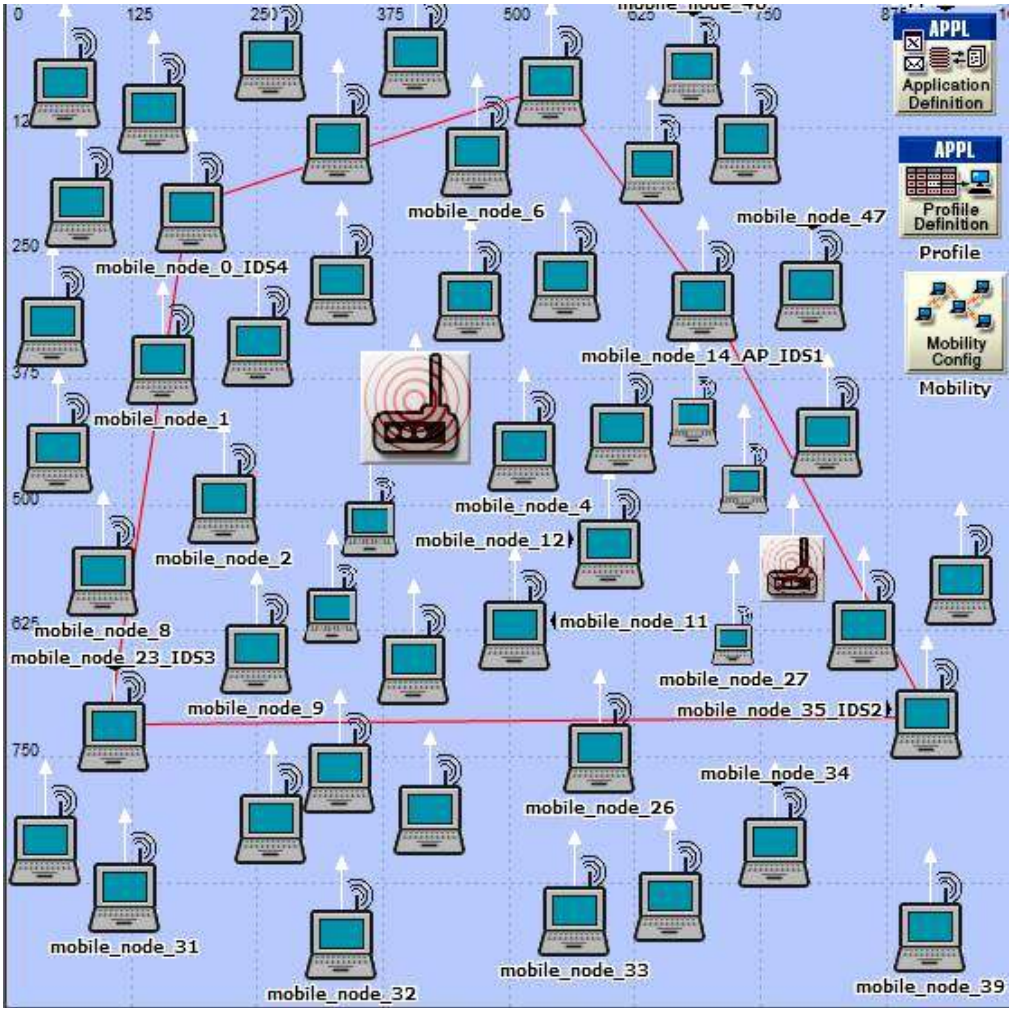


**Figure 3.** Proposed scenario.

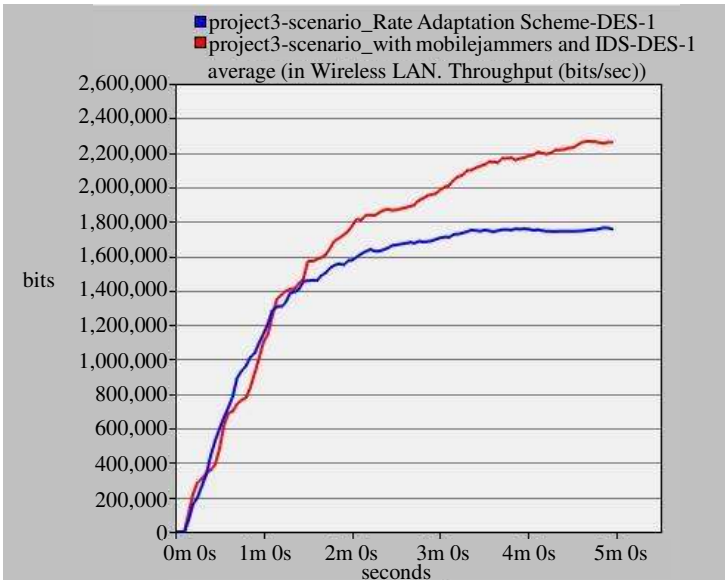


**Figure 4.** Average WLAN throughput comparison between two methods.

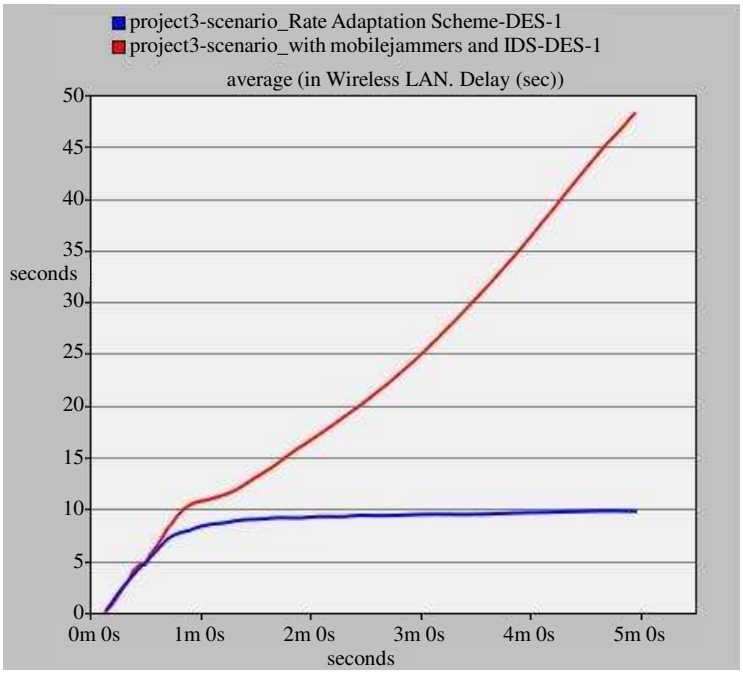


**Figure 5.** Average WLAN comparison between two methods.

received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer.

As it is indicated on **Figure 5**, USM mechanism contains high rate of delay according to the proposed method. Since USM sends the packets on different path by detour the jamming area, it has high average end-to-end delay due to increasing number of hops for the data transmission. The one of the drawbacks of USM is high rate of delay due to high rate of security which increases number of hops. The Rate adaptation scheme relays the entire process to PDR values since these values can be affected due to mobility of nodes and working mechanism that may lead to redundant power consumption.

## 6. Conclusion

The use of MANET technology has increased significantly and security becomes critical problem since a variety of research efforts were spent on vulnerabilities of MANET that concerns the security against DoS attacks that are launched against mobile nodes easily. Both USM and RAS are two different proposed mechanisms that are compared in terms of specific performance metrics in this research and both techniques have pros and cons on detecting and mitigating Jamming attacks. A network-wide protection is required for the MANET and unified security solution is a great deal to protect both route and data forwarding operations in the data link layer. The RAS and USM mechanisms can be combined or implemented on specific mobile nodes by creating guard node selection process with different network deployment architectures. Researchers have proposed USM and RAS mechanisms in order to provide strong defence against DoS attacks. Future studies should consider dynamic structure of mobile networks and different communication protocols to provide network-wide protection with proposed mechanisms.

## References

[1] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc*, *Sensor and Ubiquiotus Computing*, **3**, 79-94. http://dx.doi.org/10.5121/ijasuc.2012.3306

[2] Ju, K. and Chung, K. (2012) Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi Hop Tactical Networks. *International Journal of Security and Its Applications*, **6**, 149-154.

[3] Nguyan, D., Zhao, L., Uisawang, P. and Platt, J. (2000) Security Routing Analysis for Mobile Ad-Hoc Networks. Interdisciplinary Telecommunications Program of Colorado University.

[4] Habib, A., Hefeeda, M. and Bhargava, B. (2003) Detecting Service Violations and DoS Attacks. *The* 10*th Annual Network and Distributed System Security Symposium*, San Diego, 177189.

[5] Lackner, G. (2013) Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi, and WiMAX. *International Journal of Network Security*, **15**, 420-436.

[6] Jain, R. and Nguyen, T. (2009) A Survey of WiMAX Security Threats. Project Report.

[7] Li, W.J., Parker, J. and Joshi, A. (2012) Security through Collaboration and Trust in MANETs. *Mobile Networks & Applications*, **17**, 342. http://dx.doi.org/10.1007/s11036-010-0243-9

[8] Samreen, S. and Narasimha, G. (2013) An Efficient Security Mechanism to Detect Packet Droppers in a MANET under Individual and Collusive Adversarial Models. *International Journal of Computer Applications*, **82**, 39.

[9] Mandal, J.K. and Lutful Hassan, K. (2013) A Novel Technique to Detect Intrusion in MANET. *International Journal of Network Security & Its Applications*, **5**, 179. http://dx.doi.org/10.5121/ijnsa.2013.5515

[10] Padmaja, G.M. and Lakshmi, Ch.R. (2012) Analyzing the Detection of Active Attacks in Wireless Mobile Networks. *International Journal of Reviews in Computing*, **9**, 34.

[11] Shah, V. and Modi, N.K. (2012) A Comparative Analysis of Network Layer Threats & Defense Mechanisms of MANETs. *International Journal of Advanced Research in Computer Science*, **3**, 160.

[12] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocols's Performance in Mobile Ad Hoc Networks. *International Journal of Science and Advanced Technology*, **2**, 188-191.

[13] Xu, W., Trappe, W., Zhang, Y. and Wood, T. (2005) The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. *Proceedings of* 6*th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Illinois, 25-27 May 2005.

[14] OPNET Corporation www.opnet.com

[15] Cavin, D., Sasson, Y. and Schiper, A. (2002) On the Accuracy of MANET Simulators. *Proceedings of the* 2*nd ACM International Workshop on Principles of Mobile Computing*, ACM Press, Toulouse, 38-43. http://dx.doi.org/10.1145/584490.584499

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.