Enhancement of Routes Performance in MANET Avoiding Tunneling Attack

Pushpendra Niranjan
Department of Information Technology
LNCT (RGPV),Bhopal, M.P. India

Manish Shrivastava
Department of Information Technology
LNCT (RGPV),Bhopal, M.P. India

Rajpal Singh Khainwar
Department of Computer Science & Engg.
RRIT (RGPV),Bhopal, M.P. India

ABSTRACT

MANET consists of spatially distributed autonomous small devices which creates a self connected environment. MANETs are originally motivated by military applications such as border surveillance and battlefield monitoring; today MANET can be used in many civilian applications, including home automation, healthcare, traffic control and habitat/environment monitoring. basic security services of MANET include authentication, confidentiality, integrity, anonymity and availability. However, in contrast to traditional wireless networks, in MANET [1], physical security of sensor nodes are not granted as they are usually deployed in remote and hostile environments. Therefore, attackers can easily compromise sensor nodes and use them to degrade the network's performance. Due to lack of physical security, the existing security solutions that are developed for traditional wireless networks cannot be directly employed in MANET. The security requirements of many protocols changed the situation and a more detailed research is currently underway to develop secure ad hoc routing protocols. MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. This paper focuses on wormhole based attacks and their detection mechanisms are analyzed. In this paper we specifically considering Tunneling attack which do not require exploiting any nodes in the network and can interfere with the route establishment process. Instead of detecting suspicious routes as in previous methods, we implement a new method which detects the attacker nodes and works without modification of protocol, using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions. The proposed work is simulated using OPNET-14, and results showing the advantages of proposed work.

General Terms

Authentication, confidentiality, integrity, availability, time

delay analysis, hop-count analysis, OPNET-14.0 simulation.

Keywords

Sensor node, Tunneling attack, Battlefield monitoring,

Habitat/environment, protocols, MANET.

1. INTRODUCTION

A MANET[1][2] is a mobile mesh topology that consists of wireless sensor nodes that dynamically self organized connected by wireless links. Vehicular ad hoc networks and Sensor ad hoc networks are the varieties of MANETs. See in Figure 1.1.

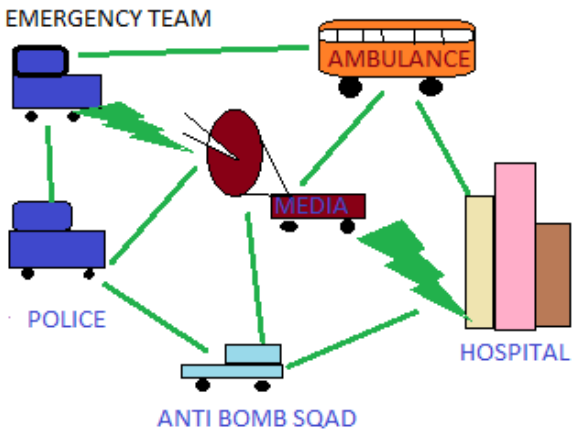

Fig: 1.1 Ad-hoc Network

MANETs are originally motivated by military applications such as border surveillance and battlefield monitoring; today MANET can be used in many civilian applications, including home automation, healthcare, traffic control and habitat/environment monitoring. basic security services of MANET include authentication, confidentiality, integrity, anonymity and availability. WSNs also as a special case of Mobile Ad-Hoc Networks (MANETs) are originally motivated by military applications such as border surveillance and battlefield monitoring; today WSNs can be used in many civilian applications, including home automation, healthcare, traffic control and habitat/environment monitoring. Wireless Sensor Networks have several unique characteristics that make them distinguishable from traditional wireless networks. First of all, WSNs generally operate in unattended areas and contain a large number of sensor nodes, which can be in the order of thousands. These nodes have strictly limited resources in terms of energy, memory, communication and computation. Due to such resource constraints, reliability and precision of a single sensor node is significantly low thereby requiring collaborative data collecting and processing. In addition, because of the simple and unreliable hardware,

sensor nodes may die earlier than their expected lifetime. Hence, the number of sensor nodes may be changed in the network lifetime in a dynamic topology. In order to use WSNs in real world applications, these unique characteristics must be carefully addressed during the protocol design.

A typical wormhole attack (Tunneling attack) [3] requires two or more attackers - malicious nodes - who have better communication resources than regular sensor nodes. The attacker creates a low-latency link (i.e. high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries. Once the tunnel is established, the attacker collect data packets on one end of the tunnel, sends them using the tunnel (wired or wireless link) and replays them at the other end see in figure 1.2.

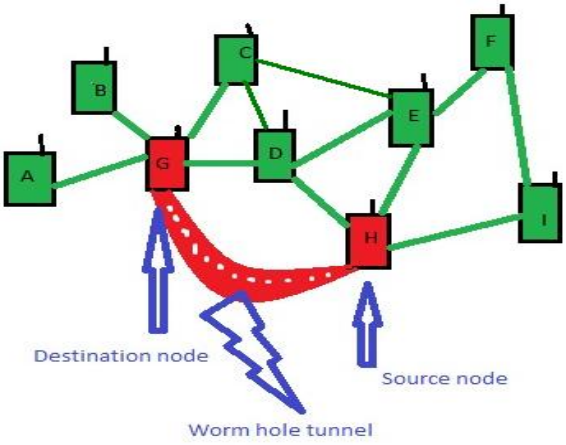

Fig: 1.2 Tunneling effect

These attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as AODV/ DSR, the attack could prevent the discovery of any routes other than through the wormhole.

1.1 Categories of N/W Attack

In security N/W, attacks are two types; active attacks and passive attacks. Wormhole attack [3] comes under active attack category is depicted in Figure1.3.

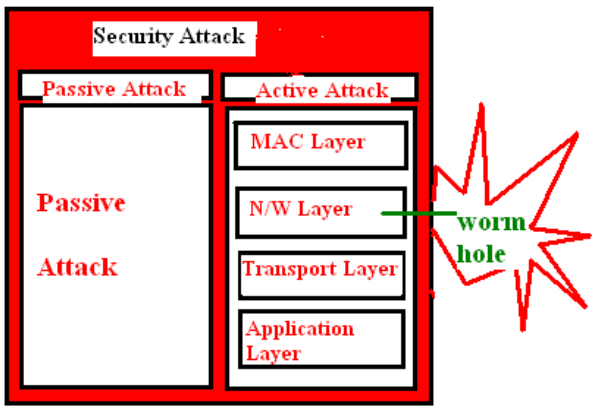

Fig: 1.3 Categories of attack

1.2 Variants of Wormhole Attacks

Several attacks that are similar or related to wormhole attacks exist in MANETs [4][5][6].

1.2.1 Spoofing

In spoofing (or impersonation) attacks, the attacker takes the identity of another node in the network and hence, all the messages directed to that victimized node are received by the attacker.

1.2.2 Black-hole

In a black-hole attack, a malicious node makes itself a part of many routes and drops all data packets transmitted over those routes.

1.2.3 Gray hole

In order to reduce the probability of detection, the malicious node can mount a more intelligent attack, called gray hole, in which it selectively drops the data packets.

1.2.4 Sinkhole

In sinkhole attacks, malicious nodes either change or do not relay the received data to its destination so that the performance of the network is reduced. If the sinkhole attack targets a specific source node, it may affect the availability of the victim node.

This paper focuses on wormhole attacks detection and avoiding tunneling effect .In this paper section 1 presents the effect of tunneling attack (worm hole) in the MANET and attack is used against on demand routing protocol.The rest of the paper is organized as follows. Section 2 presents the categories of wormhole and other related security attacks and basic description of paper. Section 3 provides a related work with wormhole attacks, whereas in Section 4, we discuss proposed method and The results and open research areas are discussed in Section 5. Finally, concluding remarks are made in Section 6.

BASIC DESCRIPTION

1.3 Problem Statement

In wireless network many types of attacks can be initiated but most of them are relative easy to detect because of their property of dramatically altering the network statistics but one different type of attack we consider in this paper. it is very important when considering security issues of network, is wormhole attack, which is difficult to detect & can harm by directing important data to unauthorized nodes. During the route discovery process, a wormhole can relay route request and response messages between distant nodes, creating the appearance of shorter routes to destinations. Since the wormhole can be anywhere along a route, a source will have to detect its existence somewhere along the route when a node sets up the route (on-demand).

1.4 Goal

The goal of this paper is to evaluate the effectiveness and efficiency of secure routing protocols in MANET using case study with existing attack patterns in ad hoc environment based on the literature study and wormhole attack is always a problem for detection efficiently with non hardware approach. In this paper we try to implement a technique which can efficiently detect this attack and avoid them.

1.5 Purpose

In this paper we specifically considering Wormhole attack which does not require exploiting any nodes in the network

and can interfere with the route establishment process. Instead of detecting suspicious routes as in previous methods, we implement a new method which detects the attacker nodes and works without modification of protocol, using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions.

2. LITERATURE REVIEW

2.1 Distance-bounding/Consistency-based Approaches

The majority of researchers try to prevent wormholes using distance-bounding techniques, which allow two communicating sensor nodes to estimate the actual distance between them. Distance-bounding techniques can be based on message traveling time information, directional antennas or geographical information. These techniques generally require specialized hardware and therefore they may be considered impractical for certain networks.

Message travelling time information is usually expressed in terms of round trip time (RTT). One way to prevent wormhole attack, as used by Hu *et al*. [7] , Tun and Maw [8] Chiu *et al*.

In [8], Tun and Maw propose a wormhole detection algorithm that is based on both the neighbor-numbers-based mechanism and RTT mechanism. The first consideration is based on the fact that by introducing new links into the network, the adversary increases the number of neighbors of the nodes within its radius. The second consideration is that the transmission time between two effected nodes is considerably higher than that between two normal neighboring nodes. This system does not require any specific hardware.

Authors of [9]proposes a transmission-time-based mechanism (TTM) to detect wormhole attacks during the route setup procedure by computing transmission time between every two consecutive sensor nodes along the established path. Wormhole is identified based on the fact that the transmission time between two fake neighbors created by wormhole is considerably higher than that between two real neighbors, which are within radio range of each other. Similar to [8], there is no special hardware requirement for TTM mechanism.

2.2 Geographical / Temporal Leashes

In [10] and [7] , the authors proposed a wormhole detection protocol that restricts the maximum transmission distance of data packets. It is assumed that a node can obtain a key for any other node. Authentication is applied to each data packet to introduce the concept of geographical and temporal packet leashes for detecting wormholes. In the geographic packet leash, when node A sends a packet to another node B, the node must include its location information and sending time into the packet. Node B can estimate the distance between them. The geographic leash computes an upper-bound on the distance. In the temporal leashes, all nodes must have tight time synchronization. The temporal leash ensures that a packet has an upper-bound on its lifetime. The maximum difference between any two nodes' clocks is bounded by a predetermined threshold and this threshold value must be known to all the nodes. By using the threshold value, sensor nodes are able to check the expiration time of data packets and determine whether there is a wormhole attack in place. If the receiving time of a packet exceeds the packet expiration time, the packet is discarded.

2.3 Synchronized Clock-based Solutions

Synchronized clock-based solutions assume that all sensor nodes in the network are tightly synchronized and each data packet includes the time at which it is sent out. The main idea behind these solutions is that when a data packet is received, the receiver node compares the receiving time with the time at which the packet is sent out. As the receiver node has the knowledge of transmission distance and consumed time, it is able to detect if the packet has traveled too far. If the transmission distance is far beyond the maximum allowed travel distance, probably the network is under a wormhole attack.

In order to avoid the problem of using special hardware for time synchronization, an RTT mechanism is proposed by Zhen and Srinivas [11]. The RTT is the time that extends from the RREQ sending time of a node A to route-reply message (RREP) receiving time from a node B by node A. When node B receives an RREQ, it will check the RTT. If the RTT exceeds a threshold, the RREQ will be dropped. However, it implies that the routing messages cannot be altered and all nodes are time synchronized, and a key pair exists between any node pair. A will calculate the RTT between A and all its neighbors. Because the RTT between two fake neighbors is higher than two real neighbors, node A can identify both the fake and real neighbors. In this mechanism, each node calculates the RTT between itself and all its neighbors. This mechanism does not require any special hardware and it is easy to implement; however, it cannot detect exposed attacks because fake neighbors are created in exposed attacks.

2.4 Trust-based Solutions

Ozdemir *et al*. [12]proposed a time and trust-based wormhole detection mechanism. The proposed technique combines a time-based module with a trust-based module to detect compromised nodes that send false information. These two systems run in parallel. Time-based module acts in three steps: in the first step, neighboring nodes are specified for each node. In the second step each node finds the most appropriate path to the base station. Finally, in the third step, the algorithm investigates whether there is wormhole in the network. Malicious nodes on the path can mislead the time-based module by providing incorrect information. To prevent this problem, trust-based module constantly observes the first module and calculates trust values of neighbor nodes. These values are used to modify the path next time. Pirzada and Mcdonald [13] deviate from the customary strategy of using cryptography and instead use a trust-based scheme that is influenced by the human behavioral model. They applied a trust scheme to the DSR protocol[14] to detect sinkhole and wormhole attacks in a sensor network. This system requires the nodes to operate in a promiscuous mode. They use inherent features of DSR protocol to compute trust level in neighbor nodes. In this system, each node must execute the trust model, measures the sincerity of its neighbor nodes by monitoring their participation in the packet forwarding mechanism. The source node verifies the different fields in the forwarded IP packet for requisite modifications through a sequence of integrity checks. If the forwarding node does not transmit the packet at all, its trust measure is decremented. Similarly, if the integrity checks succeed, it confirms that its direct trust counter is incremented.

3. PROPOSED WORK

We have performed the simulation of the proposed scheme in Opnet Network Modeler 14.0 to prove practical efficiency of the scheme; the physical parameter considerations are same as taken in mathematical modeling. The steps of modeling in

FSM (Finite State Machine) of Proposed Algorithm are as follows:

Step1. Randomly Generate a Number in between 0 to maximum number of nodes.
Step2. Make the Node with same number as transmitter node.
Step3. Generate the Route from selected transmitting node to any destination node with specified average route length.
Step4. Send packet According to selected destination and start timer to count hops and delay.
Step5. Repeat the process and store routes and their hops and delay.
Step6. Now if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker.
Step7. Now check the delay of all previous routes which involve any on node of the suspicious route. Now the node not encounter previously should be malicious let there are N such nodes.
Step8. In N == 1 then it is the attacker else wait for future sequences which shows deviation and involve only one of N nodes.
Step9. These nodes are black listed by the nodes hence they are not involved in future routes.
Step10. Whole process (from step1 to step9) is repeated until we didn't get the specified goal (goal can be).
1. To get complete list of malicious nodes.
2. To run for specified time.
3. To run for specific number of packets etc.

4. SIMULATION RESULT

For the simulation we have created node models, process models, & packet models, we also used some predefined node models from library. The details of models with their technical parameters are as follows

Total Nodes = 36
Applying protocol= DSR
Packet size = 1024 bits constant
Packet inter arrival time = 1sec. constant
Data Rate = 11 Mbps.
Area = 10 square Km.
Destination Address = Random.
Modulation = BPSK
Antenna = Omni Directional

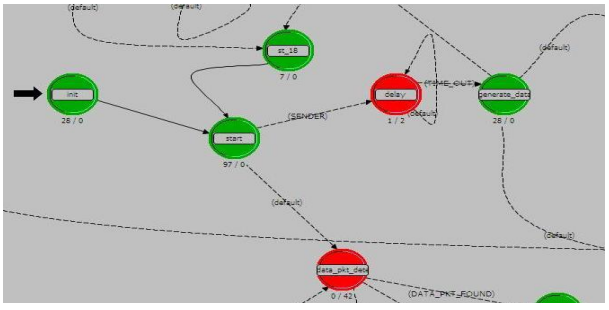

Fig: 4.1 Part of Complete Process Model showing only entering process & decision making branches for sender or receiver.

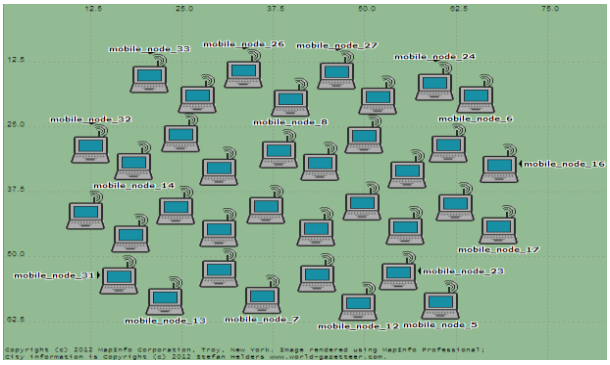

Fig : 4.2 Node distribution without attack

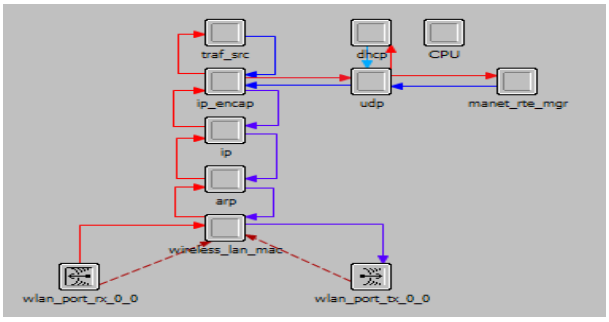

Fig : 4.3 internal architecture of node

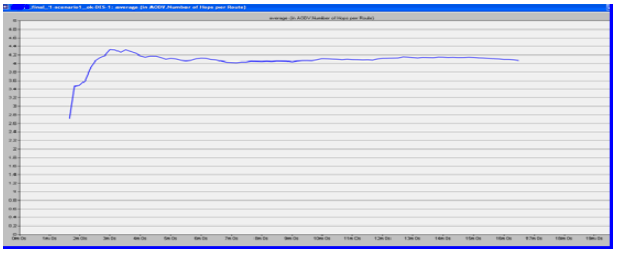

Fig : 4.4 Average hop count per route (4-4.5)

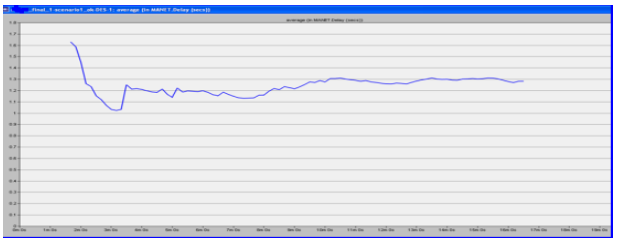

Fig : 4.6 Average time delay per route (1-1.5 sec)

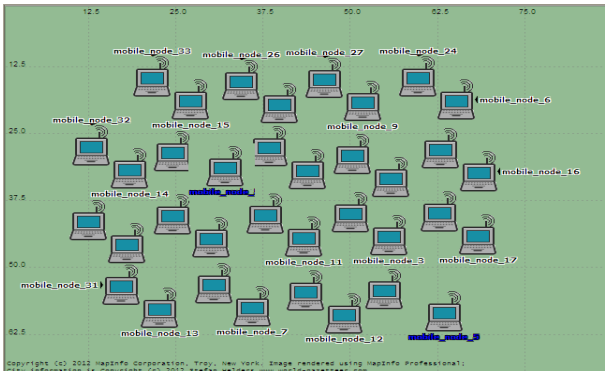

Fig : 4.7 Two nodes with applying attack

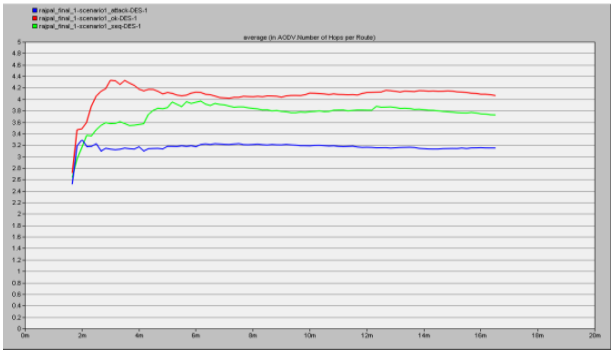

Fig: 4.8 Average Hop count per route comparison.

Attack reduces the average hop count by 20% (shown in blue) from normal condition (shown in red) which shows the selection of attaching node in route, the proposed algorithm significantly regains the hop counts by avoiding the attacker (shown in green)

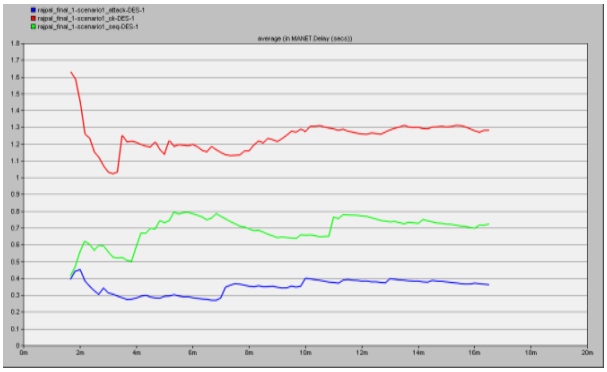

Fig: 4.9 Average delays per route comparison.

Attack reduces the average delay by 75% (shown in blue) from normal condition (shown in red) which shows the shorting of route by attacking route, the proposed algorithm have much better delay which presents the elimination of attacker (shown in green).

5. CONCLUSION

Wormhole attacks in MANET can significantly degrade network performance and threaten network security. In wormhole attacks, find out suitable routes for sending data packet to the destination is quite complicated. In this paper, we presented the categories of N/W Security attacks where wormhole attack exist. After describing some N/W attack which is similar as a wormhole attack, we analyzed problems statement , objective and purpose related with the network security, The wormhole attack is especially harmful against many ad-hoc routing protocols for example, ad hoc on-demand distance vector (AODV), dynamic source routing (DSR). In the next section of this paper provided a number of wormhole detection techniques, each technique has its own weakness and there is no wormhole detection technique that can detect wormhole attacks completely. Finally, by analyzing multipath algorithm which is based on the hop count and time delay analysis, we presented the open research issues in the wormhole detection area.

6. REFERENCES

[1] A. Akyildiz, I.F. Su, W. Sankarasubramaniam, and E. Cayirci. "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102−114, Aug. 2002

[2] S. Hadim and S.N. Mohamed. "Middleware challenges and approaches for wireless sensor networks," *IEEE Distributed Systems*, vol. 7, no. 3, pp. 1−23, Mar. 2006.

[3] Hu, Y.C.; Perrig, A.; Johnson, D.B. Wormhole Attacks in Wireless Networks. *IEEE J. Sel. Area Comm.* 2006, 24, 370–380.

[4] S.Pal, A.K. Mukhopadhyay, and P.P. Bhattacharya. "Defending mechanisms against sybil attack in next generation mobile ad-hoc networks," *ITEE Technical Review Journal*, vol. 25, no. 4, pp. 209−14, Jul-Aug. 2008.

[5] J.R. Douceur. "The sybil attack," Proceedings of the *International Workshop on Peer-to-Peer Systems*, pp. 251−60, Mar. 2002.

[6] D. Glynos, P. Kotzanikolaou, and C. Douligeris. "Preventing impersonation attacks in MANET with multi-factor authentication," Proceedings of the Third *International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, pp. 59−64, Apr. 2005

[7] Y.C. Hu, A. Perrig, and D.B. Johnson. "Packet leashes: A defense against wormhole attacks in wireless ad-hoc networks," Proceedings of *22nd IEEE INFOCOM*, pp. 1976−86, Apr. 2003

[8] Z. Tun and A.H. Maw. "Wormhole attack detection in wireless sensor networks," Proceedings of *World Academy of Science Engineering and Technology*, vol. 46, pp. 545−50, Dec. 2008.

[9] K.U. Khan, A.V. Reddy, R.U. Zaman, K.A. Reddy, and T.S. Harsha. "An efficient DSDV routing protocol for wireless mobile ad-hoc networks and its performance comparison," Second *UKSIM European Symposium on Computer Modeling and Simulation*, pp. 506−11, Sep. 2008.

[10] Y.C. Hu, A. Perrig, and D.B. Johnson, "Wormhole detection in wireless ad-hoc networks," *Department of Computer Science, Rice University, Technical Report* TR01-384, Jun. 2002

[11] J. Zhen and S. Srinivas. "Preventing replay attacks for secure routing in ad-hoc networks," Proc. of 2nd *Ad Hoc Networks and Wireless*, pp. 140−50, 2003.

[12] S. Özdemir, M. Meghdadi, and Ý. Güler. "A time and trust based wormhole detection algorithm for wireless sensor networks," (manuscript in Turkish), in 3rd *Information Security and Cryptology Conference* (ISC'08), pp. 139−4, 2008.

[13] A.A. Pirzada and C.S. McDonald. "Circumventing sinkholes and wormholes in ad-hoc wireless networks," Proceedings of *International Workshop on Wireless Ad-hoc Networks*, London, England, Kings College, London, 2005

[14] D.B. Johnson, D.A. Maltz, and Y. Hu. "The dynamic source routing protocol for mobile ad-hoc networks," *IETF MANET, Internet Draft. Available from*: http://www.cs.cmu.edu/~dmaltz/internet-drafts/draft-ietf-manet-dsr-09.txt [last cited in 2003].