Performance Analysis of Worm-Hole Attack in Wireless Sensor Network using AODV Routing Protocol

Shweta Dalke [1] , Pallavi Pahadiya [2]
[1](Electronics & Communication/ Truba College of Engineering & Technology/ RGPV,Bhopal, ,INDIA)
[2](Electronics & Communication/ Truba College of Engineering & Technology/ RGPV,Bhopal, ,INDIA)

Abstract

Wireless sensor networks continue to grow, and becoming a very popular technology, so it needs some effective security mechanisms. In sensor networks, sensor nodes interact with the sensitive data and operate in hostile environments. The wireless sensor networks are being used in many ways. Traditionally, it has been used in the high-end application such as radiation and nuclear-threat detection systems, weapons sensors for ships, biomedical applications, habitat sensing and seismic monitoring The wormhole attack is also one of the severe attacks of WSN. The wormhole attack is basically launched by a pair of collaborating nodes. In wormhole attack two collaborating attacker nodes occupy strong strategic locations in two different parts of the network and advertise to have the shortest path for transmitting data and make wormhole tunnel.. This paper discusses some of the techniques put forwarded by researchers to detect and prevent worm hole attack in WSN using QualNet simulator.

Keywords: *WSN ,worm hole attack,QualNet, Malicious Node.*

I. INTRODUCTION

Sensor networks often have one or more points of centralized control called base-stations. A base station is typically a gateway to another network, a powerful data processing or storage centre, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. In some previous work on sensor network routing protocols, base stations have also been referred to as sinks.

Base stations are typically many orders of magnitude more powerful than sensor nodes. They might have workstation or laptop class processors, memory, and storage, AC power, and high bandwidth links for communication amongst themselves. However, sensors are constrained to use lower-power, lower-bandwidth, shorter-range radios, and so it is envisioned that the sensor nodes would form a multi-hop wireless network to allow sensors to communicate to the nearest base station. [1].

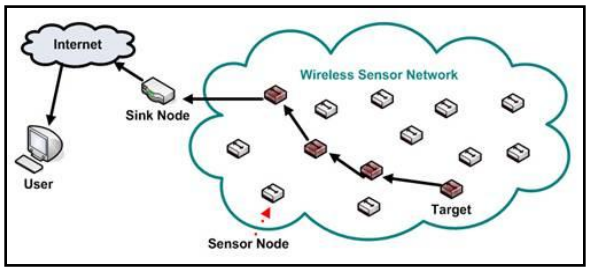

Figure1 .1: Simple Wireless Sensor Network

II. WORMHOLE ATTACK

A. *Wormhole Attack*

A typical wormhole attack requires two or more attackers (malicious nodes) who have better communication resources than regular sensor nodes. The attacker creates a low-latency link (high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighbouring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries Once the tunnel is established, the attackers 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.

1) *Types of Wormhole Attack*

Wormhole attack can be launched by using various techniques in wireless networks. These are as follows [2]:

***a) Wormhole Using Encapsulation*:** In encapsulation-based wormhole attacks, several nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Since encapsulated data packets are sent between the malicious nodes, the actual hop count does not increase during the traversal. Hence, routing protocols that use hop count for path selection are particularly susceptible

to encapsulation-based wormhole attacks. For example, ad-hoc on-demand distance vector (AODV) routing protocol, a source initiated on on-demand routing protocol, is one of the most popular routing protocols in WSNs. In AODV protocol, in order to limit the amount of flooding, each node broadcasts only the first route request (RREQ) message it receives and drops any further copies of the same request. However, AODV protocol fails under encapsulation-based wormhole attacks. When a malicious node at one part of the network hears the RREQ, it transmits this RREQ to the other malicious node at a distant location near the destination. The second malicious node then rebroadcasts the RREQ. The neighbours of the second malicious node receive the RREQ and drop any further legitimate RREQs that are coming from legitimate multi-hop paths. As a result, the route between the source and the destination include the malicious nodes that form the wormhole. This prevents sensor nodes from discovering legitimate paths that are more than two hops away.

b) Wormhole Using High-quality/Out-of-band Channel*:* In this mode, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. This tunnel can be achieved, for example, by using a direct wired link or a long-range directional wireless link. This mode of attack is more difficult to launch than the packet encapsulation method since it needs specialized hardware capability.

c) Wormhole using High Power Transmission: In this type of wormhole attack, only one malicious node with high-power transmission capability exists in the network and this node can communicate with other normal nodes from a long distance. When a malicious node receives an RREQ, it broadcasts the request at a high power level. Any node that hears the high-power broadcast rebroadcasts the RREQ towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of another malicious node. This attack can be mitigated if each sensor node is able to accurately measure the received signal strength.

d) Wormhole Using Protocol Distortion*.:* In this mode of wormhole attack, one malicious node tries to attract network traffic by distorting the routing protocol. Routing protocols that are based on the 'shortest delay' instead of the 'smallest hop count' is at the risk of wormhole attacks by using protocol distortion. In hop-count-based routing protocols, in order to reduce the number of MAC-layer collusions, sensor nodes typically wait for a random time before RREQ forwarding. In this wormhole mode, a malicious node can create a wormhole by not forwarding RREQs without back-off. The purpose is to let the RREQ packet arrive first at the destination and so that the malicious node is included in the path to the destination. This kind of wormhole by itself is harmless and it is also called "rushing attack" in the literature. However, in many circumstances, attackers use this attack as an initial step to perform denial-of-service attacks, which can compromise the security of the entire network.

e) Wormhole Using Packet Relay: Packet-relay-based wormhole attacks can be launched by one or more malicious nodes. In this attack type, a malicious node relays data packets of two distant sensor nodes to convince them that they are neighbours. This kind of attack is also called "replay-based attack" in the literature.

III. SIMULATION AND PERFORMANCE ANALYSIS

A. Simulation of Wireless sensor networks**:** The simulation of the wireless sensor network consists of three main scenarios. The configuration of scenarios is based on the number of nodes are deployed and the position of the source node and destination node. Initially all sensor nodes in each scenario are normal and no malicious node is present in the scenario. The standard AODV routing algorithm is used at routing protocol on network layer. The scenarios are differentiated on the basis of number of nodes present in the scenario and the nodes are deployed in a manner that they are in the range of other nodes. On the basis of scenarios the result are obtained. Each scenario simulated in two cases, these are:-

Normal scenario: In normal scenario all the nodes have same transmission power. The value of the MY-A integer variable is set before the simulation runs, this value is change at the node in scenarios. If the value of MY-A at the node is 4 than this node become a malicious node in the network. In normal scenario the value of MY-A is equals to 1 at every node in networks deployment phase. There is an assumption in the network deployment phase that in the beginning all the nodes are normal and non malicious. The source node sends the packets to the destination node through intermediate nodes in the routing path.

Scenario with malicious node: This is a next step after a normal node deployment in the scenario. In these scenarios wormhole attack is implemented. The value of transmission power of two nodes is higher than the other nodes means these two nodes have a high range of propagation distance and they communicate with each other from the long distance. One of these nodes is malicious node means the value of MY-A is 4, so it

become a attacker node in the networks and those node which has a value of MY-A=4 dropped the data packets sends by the source node to destination node. Routing path in between the source and the destination is the shortest path within the network and attacker node is a intermediate node in the routing path. Attacker nodes are always trying to drop all the packet comes from the source node.

Scenario 1

i. Sensor network with 8 mobile nodes and statically placed.
ii. IEEE 802.15.4 wireless standard for PHY and MAC.
iii. AODV routing protocol for sensor nodes.
iv. All nodes are fully. Functional device (FFD).
v. Network protocol IPv4 is used at nodes.

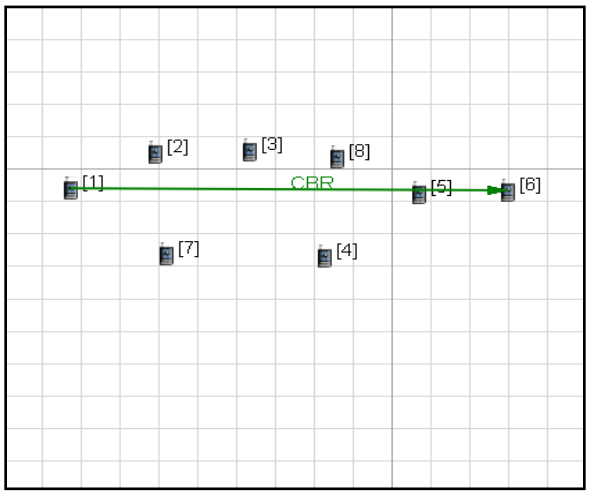

Figure:3.1 Scenario-1

Figure 3.1 shows the scenario-1. The CBR traffic generator is from the node-1 to node-6 means node-1 wants to send the data packets to the node-6. Other nodes are the intermediate nodes in between the source node and destination node. Initially the source node finds a route for the destination node so it broadcast the route request packet. The neighbour node received the request packet.

In the above figure-3.1 nodes are deployed in the sensor network, this type scenario is used in small field such as home applications. They sensed the data in small space and that sends to other nodes. This study is based on the routing attacks in the sensor networks so take the least number of nodes in the scenario for the best results. The above topology is simple kind of topology in which all nodes sends the packets within the transmission range. The CBR stands for constant bit rate. The source and destination connect to CBR connection.

Figure 3.2 indicates route selected for sending the data packets from the source node to destination node. This route has minimum number of hops and it is a shortest path for the destination in the network.

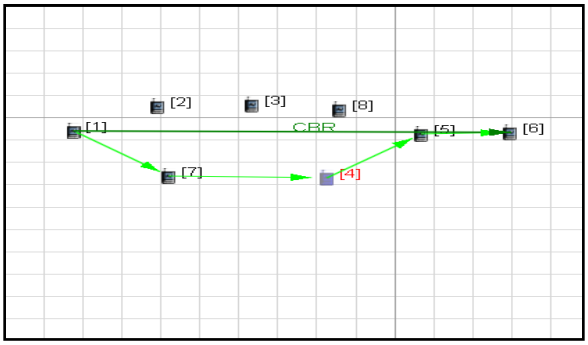

Fig-3.2 Routes Selected

The figure-3.3 shows the number of data packets sends from the source node to the destination node. The graph is generated in analysis of the scenario. In the graph the x-axis indicates the number of data packets sends and the y-axis indicates the node id.

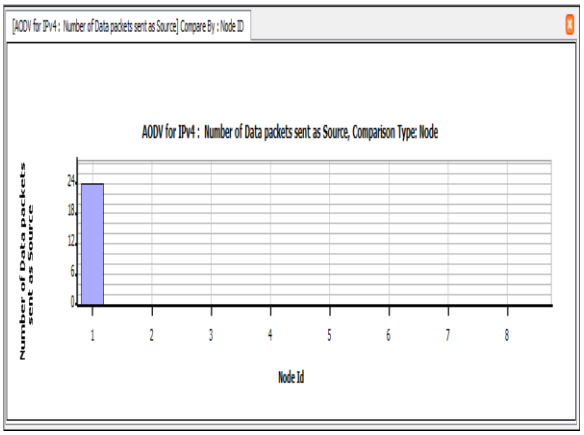

Fig-3.3 Packets Sent

The AODV routing protocol successfully implemented on the scenario-1 and the source node-1 sent the data packets to the destination node. At source node the Avg. throughput is generated.

The above figure 3.4 shows the number of data packets received by the destination node. The x-axis indicates number of data packets received and y-axis indicates the node id for received data packets.

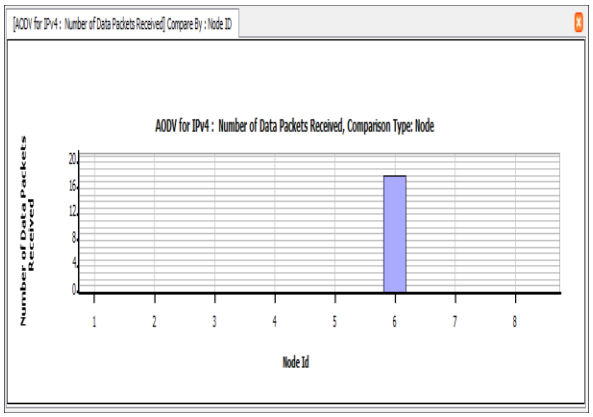

Fig-3.4 Packets Received

The data packets received by the intermediate node in routing path. If this node is destination node it received the data packets or if this node is intermediate node then forwarded the data packets to the destination node. The above figure shows that the destination node-6 received the data packets.

The figure3.5 shows the wormhole implementation in sensor networks. The node-4 is attacker node which dropped all the packets. The destination node does not receive any data packets in the presence of attacker.

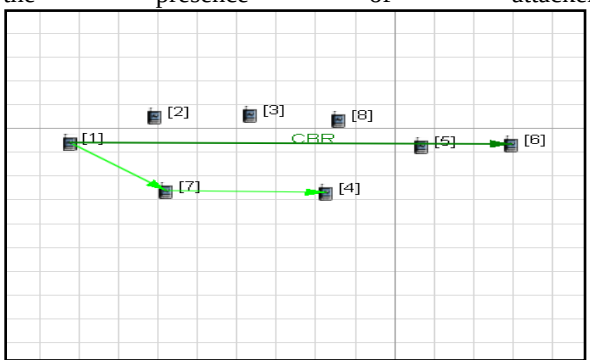

Fig-3.5 Scenario-1 with Attack

Attacker node is a part of routing path or a node somewhere in the scenario. Wormhole attacker node is in routing path and does not forward any data packets to the destination node in the networks.

In the figure 3.6, the packets dropped by the attacker node is mentioned. The x-axis indicates the number of data packets dropped and y-axis indicates the node id for the nodes in networks.

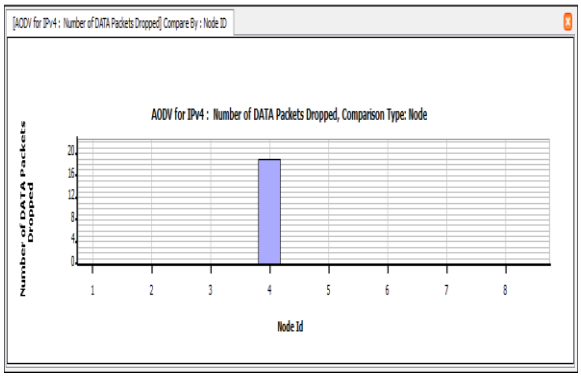

Fig-3.6 Packets Dropped

When attacker node is present in the scenario then it does not forward any data packets to the destination node. Attacker node dropped all data packets comes from the source node or an intermediate node. The destination node does not receive any data packets from the source node due to attacker node in a network.

IV. RESULTS FOR COMPARISON FOR SEVERAL NODES

A. Performance Parameters in WSN

The results of this project works is based on the three different scenarios, on the basis of these scenarios this study show that the proposed work is considerable and the results of this study are acceptable. The scenarios which are simulated in Qualnet simulator have different parameters on the basis of numbers of nodes present in the scenarios, or the number of nodes in the route path. The topologies of the scenarios are different and the attacker node deployed near the destination node each time attacker node dropped the data packets sent from the source node. The number of packets dropped more in case of malicious node and the counter measures for wormhole attacks shows that destination node still received the data packets.

1) Throughput at Source

The throughput at the source is calculated as follows:

If the session is complete, i.e., if all packets have been sent before the simulation ends, throughput = (total bytes sent * 8) / (time last packet sent - time first packet sent), where the times are in seconds. If the session is incomplete, i.e., if all packets have not been sent before the simulation ends, throughput = (total bytes sent * 8) / (simulation time - time first packet sent), where the times are in seconds.

2) Throughput at Destination

Throughput is the average rate of the successful message delivery over communication channel. The throughput is usually measured in bits per

second (bits/sec or bps) or sometimes in data packets per second or data packets per time slot
The throughput at the destination is calculated as follows:

If the session is complete, throughput = (total bytes received * 8) / (time last packet received - time first packet received), where the times are in seconds.

If the session is incomplete, throughput = (total bytes received * 8) / (simulation time - time first packet received), where the times are in seconds.

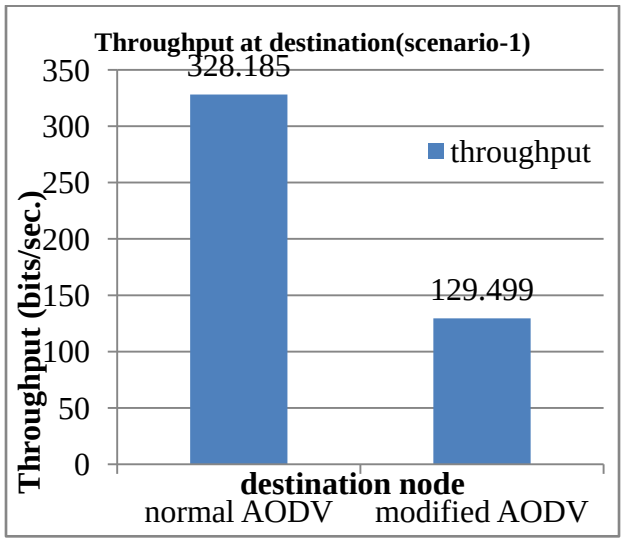

Fig. 4.1 Avg. THROUGHPUt (scenario-for 8 node)

The above figure 4.1 shows the result for scenario-1. In scenario-1, 8 sensor nodes (FFD) are deployed in the field. A pair of source and destination sent the packets to each other. The above figure analyzed on AODV routing statistics. On x-axis the figure indicates the throughput (bits/sec) and the y-axis indicates the destination on normal AODV routing protocol and modified AODV.
Compared Results

Table no.4.1 Avg. Throughputs at Destination (scenario-1)

	Normal AODV	Modified AODV
Throughput (bits/sec)	328.185	129.499

Percentage reduction in throughput

= (328.185 – 129.499) /328.125
=198.686 /328.125 * 100
=60.55%

The average reduction in the throughput at scenario-1 is 60.55 %.

*3) **Average end to end delay***

The end to end delay in network is the time taken for a packet to be transmitted across a network from source to destination. Average end-to-end delay = (total of transmission delays of all received packets) / (number of packets received), where, transmission delay of a packet = time packet received at server - time packet transmitted at client, where the times are in seconds.

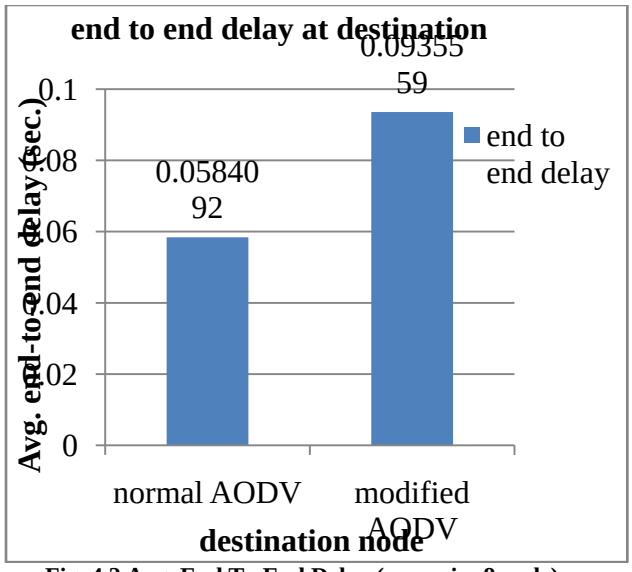

Fig. 4.2 Avg. End To End Delay (scenario- 8 node)

The above figure 4.2 shows the result for scenario-1. In scenario-1, 8 sensor nodes (FFD) are deployed in the field. A pair of source and destination sent the packets to each other. The above figure analyzed on AODV routing statistics. On x-axis the figure indicates the end-to-end delay (sec.) and the y-axis indicates the different cases on AODV routing protocol.
Compared results

Table no.4.2 Avg. end-to-end delays at destination

	Normal AODV	Modified AODV
end-to-end delay (sec)	0.0584092	0.0935559

Percentage gain in end-to-end delay

= (0.0935559 – 0.0584092)/0.0584092*100

=0.0351467/0.0584092*100

=60.80 %

The average gain in the end to end delay at scenario-1 is 60.80 %.

*4) **Average Jitter***

Average jitter is used as measure of the variability over the time of packet latency across a network. A network with constant latency has no variation (jitter). Packet jitter is expressed as an average of the deviation from the network mean latency

Average jitter = (total packet jitter for all received packets) / (number of packets received - 1) where, packet jitter = transmission delay of the current packet - transmission delay of the previous packet. Jitter can be calculated only if at least two packets have been received.

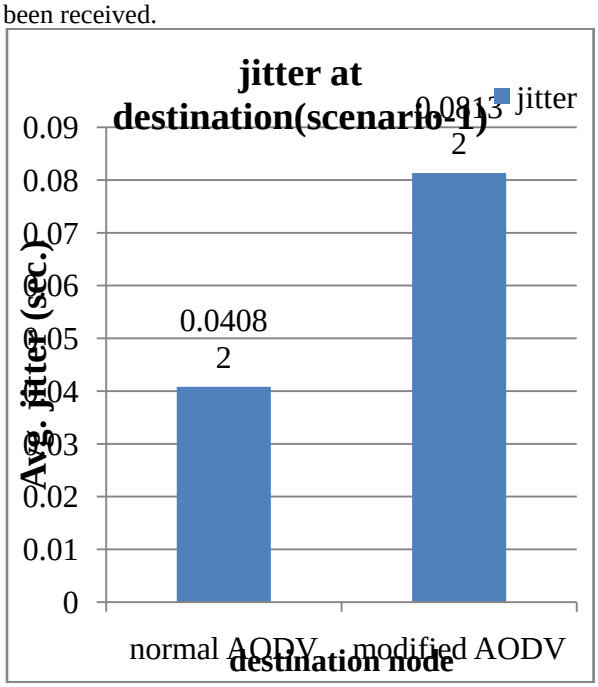

Fig. 4.3 Avg. Jitter (scenario-8 node)

The above figure 4.3 shows the result for scenario-1. In scenario-1, 8 sensor nodes (FFD) are deployed in the field. A pair of source and destination sent the packets to each other. The above figure analyzed on AODV routing statistics. On x-axis the figure indicates the Avg. jitter (sec.) and the y-axis indicates the different cases on AODV routing protocol. Compared results

Table no 4.3 Avg. Jitters at Destination

	Normal AODV	Modified AODV
Avg. Jitter(sec)	0.04082	0.08132

Percentage gain in jitter

= (0.08132 – 0.04082)/0.08132*100

= 0.0405/0.04082*100

=99.21 %

The average gain in the jitter at scenario-1 is 99.21 %.

V. CONCLUSION

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in WSN theoretically and through simulation. This research work proposed technique namely modified AODV for wormhole attack. To evaluate the performance of proposed techniques, simulation of wormhole attacks along with the simulation of proposed technique had been done**.**

REFERENCES

[1] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", in Elsevier's Adhoc Network Journal Special Issue on Sensor Network Application and Protocols, vol.l, issue.2-3, pp.293-315, September2003

[2] Devesh Jinwala, "Ubiquitous Computing: Wireless Sensor Network Deployment, Models, Security, Tbreats and Challenges", in National conference NCIIRP-2006, SRMIST, pp. 1-8, April 2006.

[3] Rouba EI Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, "DA WWSEN: A Defense Mechanism against Wormhole Attacks In Wireless Sensor Networks", in The Second International Conference on Innovations In Information Technology , pp. 1-10, 2005.

[4] M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In WISE, September 2002.

[5] AI-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong. Security in wireless sensor networks: issues and challenges. In Proc. of the 8th International Conference on Advanced Communication Technology, volume 2, Feb. 2006, pp. 1043-1048.

[6] Qualnet Developer Website https://www.scalable-networks.com/products/qualnet/.

[7] I. Khalil, S. Bagchi, and N.B. Shroff. "LITEWORP: A lightweight countermeasure for the wormhole attack in multi-hop wireless networks," Proceedings of the International Conference on Dependable Systems and Networks, pp. 612−41, 2005.

[8] T. Korkmaz. "Verifying physical presence of neighbors against replay-based attacks in wireless ad-hoc networks," International Conference On Information Technology: Coding and Computing 2005(ITCC 2005), pp. 704−9, 2005.

[9] Y.C. Hu, A. Perring, and D. Johnson. "Rushing attacks and defense in wireless ad-hoc network routing protocols," ACM Workshop on Wireless Security, pp. 30−40, 2003.

[10] L. Buttyan and J.P. Hubaux. "Security and cooperation in wireless networks," Cambridge University Press Textbook, Draft Ver.1.5.1, 2007.