Detecting Wormhole Attacks on Wireless Ad-hoc Networks: A Group based Approach

Nagendra Kumar
Department of CSE
Galgotias College of Engineering & Technology,
Greater Noida

Nagendra Kr. Mishra
Department of CSE
Galgotias College of Engineering & Technology,
Greater Noida

Shubham Omar
Department of CSE
Galgotias College of Engineering & Technology,
Greater Noida

Sandeep Saxena
Assistant Professor
Galgotias College of Engineering & Technology,
Greater Noida

ABSTRACT

The ad-hoc networks are the temporarily established wireless networks which does not require fixed infrastructure it is also called as infrastructure less network. There is no central control authority in ad-hoc network. Because of some flaws of ad-hoc network such as shared wireless medium and lack of any central coordination makes them more prone to attacks in comparison with the wired network. It is peer to peer network. Among all the attacks wormhole attack is the most severe attack. In this attack an attacker capture the packets at one location in the network and send it to another attacker at a distant location through tunnels which is established through different ways like packet encapsulation, using high power transmission or by using direct antennas. This tunnel between two colluding attackers is virtual and it is called as a wormhole. The wormhole attack is possible even if the attacker has not comprised any hosts, and all communication provides authenticity and confidentiality. By using the various approaches for finding the solution over wormhole attack, the dynamic information of the packets could still be modified. So in order to give more robust protection in some special scenario like battlefields, which requires highly secured information, there is need of developing some secured mechanism for wormhole detection. Taking into consideration this problem the proposed scheme is developed. This paper discusses proposed works on wormhole attack along with comparison of different wormhole detection techniques in ad-hoc wireless network.

Keywords

ad-hoc Networks, Worm Hole Attack, Wired & Wireless

Networks, Tunnel.

1. INTRODUCTION

Wireless ad-hoc networks are different from wired networks, ad- hoc uses wireless medium to communicate, do not rely on fixed infrastructure, and can arrange them into a network quickly and efficiently. In a Mobile ad-hoc Network (MANET), each node act as a router for other nodes, which allows data to travel, utilizing multi-hop network paths, beyond the line of sight without relying on

wired infrastructure. Security in such networks, however, is a great concern [1, 2, 7, 5]. The open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. Lack of centralized control authority makes deployment of traditional centralized security mechanisms difficult. Lack of clear network entry points also makes it difficult to implement perimeter-based defence mechanisms such as firewalls. Finally, in a MANET nodes might be battery-powered and might have very limited resources, which may make the use of heavy-weight security solutions undesirable [2, 3, 5,7, 4].

A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed channel link, are strategically placed at different ends of a network, as shown in figure 1. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbours, and force all communications between affected nodes to go through them. In general, ad-hoc routing protocols fall into two categories: proactive routing protocol that relies on periodic transmission of routing packets updates, and on-demand routing protocols that search for routes only when necessary. A wormhole attack is equally worse a threat for both proactive and on-demand routing protocols [3, 7, 4, 9].

When a proactive routing protocol [10] is used, ad-hoc network nodes send periodic HELLO messages to each other indicating their participation in the network. When node S sends a HELLO message, intruder I forwards it to the other end of the network, and node D hears this HELLO message. Since D can hear a HELLO message from S, it assumes itself and node S to be direct neighbours. Thus, if D wants to forward anything to S, it may do so unknowingly through the wormhole link. This effectively allows the wormhole attackers full control of the communication link.

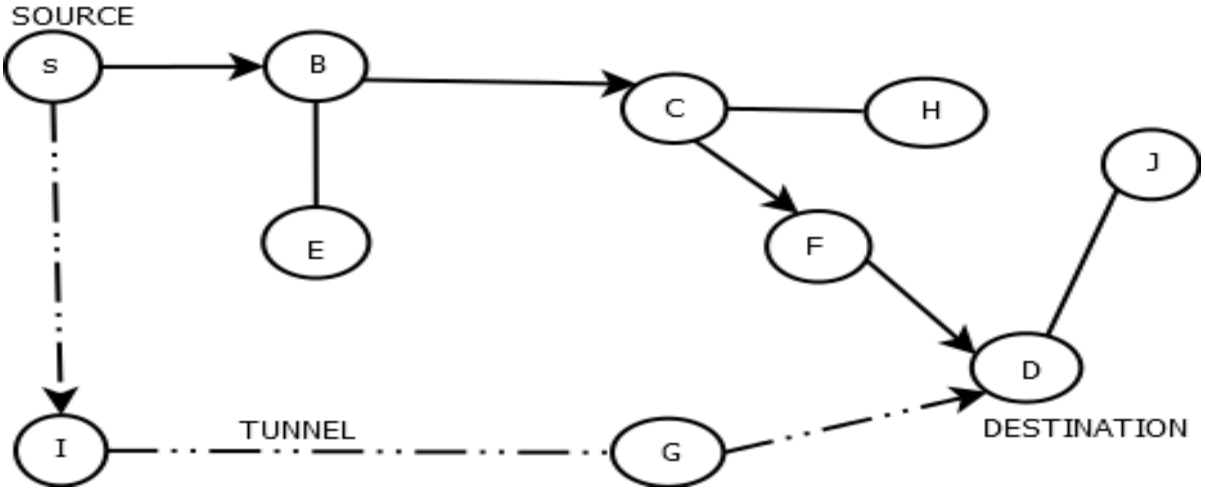

Figure 1: Wormhole attack in ad-hoc network

In case of on-demand routing protocols, such as AODV [6], when a node wants to communicate with another node, it floods its neighbours with requests, trying to determine a path to the destination. If S wants to communicate with D, it sends out a request. A wormhole, once again, forwards such request without change to the other end of the network, may be directly to node D. A request also travels along the network in a proper way, so D is lead to believe it has a possible route to node S through the wormhole attacker nodes. If this route is selected by the route discovery protocol, once again wormhole attackers get full control of the traffic between S and D. Once the wormhole attackers have control of a link, attackers can drop the packets to be forwarded by their link. They can drop all packets, a random portion of packets, or specifically targeted packets1. Attackers can also forward packets out of order or 'switch' their link on and off [3].

In this paper, an algorithm is proposed where intrusion detection has been done in a group based approach to detect the wormhole attacks. The AODV routing protocol is used as the underlying network topology. A group based approach is used for detecting whether a node is acting as a wormhole or not.

2. PROBLEM STATEMENT

In a ad-hoc network, there is main problem of security. An attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. For tunnelled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunnelled packet arrive with better metric than a normal multihop route, for example, through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

The wormhole attack is particularly dangerous against many ad-hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and, thus a neighbour of) that node. For example, when used against an on-demand routing protocol such as dynamic source routing (DSR) [11], [12] or ad hoc on-demand distance vector (AODV) [8], a powerful application of the wormhole attack can be mounted by tunnelling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbours hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST, and then discard without processing all other received ROUTE REQUEST packets originating from this same route discovery. This attack, thus, prevents any routes other than through the wormhole from being discovered, and if the attacker is near the initiator of the route discovery, this attack can even prevent routes more than two hops long from being discovered. Possible ways for the attacker to then exploit the wormhole include discarding rather than forwarding all data packets, thereby creating a permanent denial-of-service (DOS) attack (no other route to the destination can be discovered as long as the attacker maintains the wormhole for ROUTE REQUEST packets), or selectively discarding or modifying certain data packets.

3. RELATED WORK

Routing security in ad-hoc networks is often equated with strong and feasible node authentication and lightweight cryptography. A wide variety of secure extensions to existing routing protocols have been proposed over the years. However, the majority of these protocols are focused on using crypto graphical solutions to prevent unauthorized nodes from creating seemingly valid packets [5]. Unfortunately, the wormhole attack cannot be defeated by crypto graphical measures, as wormhole attackers do not create separate packets. They simply replay packets already existing on the network, which pass all cryptographic checks. Perhaps the most commonly cited wormhole prevention mechanism is 'packet leashes' by Hu et al [4]. Hu proposed to add secure 'leash' containing timing and or Global Positioning System (GPS) information to each packet on a hop-by-hop basis. Based on the information contained in a packet leash, a node receiving the packet would be able to determine whether the packet has traveled a distance larger than physically possible.

Hu proposed two different kinds of leashes: geographical leashes and temporal leashes. Geographic leashes require each node to have access to up-to-date GPS information, and rely on loose (in the order of ms) clock synchronization. When geographical leashes are used, a node sending a packet appends to it the time the packet is sent t_s and its location p_s.

A receiving node uses its own location p_r and the time it receives a packet t_r to determine the packet could have travelled. Keeping in mind maximum possible node velocity v, clock synchronization error Δ, and possible GPS distance error Δ, the distance between the sender and the receiver d_{sr} is upper-bounded by:

$$d_{sr} < \|p_s - p_r\| + 2v(t_s - t_r + \Delta) + \Delta$$

Another method of wormhole prevention techniques, somewhat similar to temporal packet leashes [10], is based

on the time of flight of individual packets. Wormhole attacks are possible because an attacker can make two far-apart nodes see themselves as neighbours. One possible way to prevent wormholes, as used by Capkun et al [14], Hu et al [15], Hong et al [13], and Korkmaz [16], is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determine whether the calculated distance is within the maximum possible communication range. The basis of all these approaches is the following. The Round Trip Travel Time (RTT)δ of a message in a wireless medium can, theoretically, be related to the distance d between nodes, assuming that the wireless signal travels with a speed of light c:

$$d = (\delta c)/2 \text{ and } \delta = 2d/c$$

The neighbour status of nodes is verified if d is within the radio transmission range R for R > d (d within transmission range): $R > \delta c/2$ and $\delta < 2R/c$. In essence, the use of RTT eliminates the need for tight clock synchronization required in temporal leashes: a node only uses its own clock to measure time. However, this approach, while accounting for message propagation, completely ignores message processing time. When a message is sent by one node and is acknowledged by another, the time it takes for a node to process a message and to reply to it is generally non-negligible, particularly in the context of bounding short distances using signals whose speed is similar to that of light in vacuum. After all, it takes the light less than 0.2 seconds to circle the entire Earth around the equator. Outstanding clock precision and practically nonexistent errors are required to bind distances on the order of hundreds of meters.

Table 1. Summary Of Wormhole Detection Algorithms

SN	RESEARCH	METHOD	COMMENTS
1	Hu et al.	Geographic and temporal leashes	GPS co-ordination of every node, Loosely synchronized clock(ms), Robust, straightforward solution, inheritance of general limitations of GPS technology.
2	Capkun et al	Packet leashes, end-to-end	GPS coordination of every node, loosely synchronized clocks(ms),Inheritance of limitations of GPS technology
3	Lazos et al.	Time of flight	Hardware enabling one-bit message and immediate replies without CPU involvement, impractical, likely to require MAC-layer modifications.
4	Park and Shin	LISP	Applicable only to static stationary networks, Impractical.
5	Hu and Evans	Directional antennas	Directional antennas on all nodes, Good solutions for network relying on directional antennas, but not directly applicable to the other networks, Several nodes equipped with both GPS and directional antennas.
6	Hu et al.	Connectivity-based approaches	Require connectivity information, Tightly synchronized clocks(ns),Impractical .
7	Song et al.	Statistical analysis	Work only with multi-path on demand protocol.
8	Weichao et al.	End to end mechanism	Require location information, loosely synchronized clocks. Mechanism uses geographic info. and authentication to detect anomaly neighbour relation.

The real problem with the wormholes is that unauthorized nodes (wormhole attackers) are able to transmit valid network messages. Techniques based on links performance may be suitable in certain cases, but they do not fully address the wormhole problem.

4. PROPOSED METHODOLOGY

Objective is to find out the malicious node that performs the wormhole attack in network. We have assumed that the MANET consists of group of nodes. The assumptions regarding the organization of the MANET are listed following section.

4.1 Proposed Architecture

The following assumptions are taken in order to design the proposed algorithm.

- A node interacts with its 1-hop neighbours directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
- Every node has a unique id in the network, which is assigned to a new node collaboratively by existing nodes.
- The entire network is geographically divided into a few disjoint or overlapping groups.
- Each group is monitored by only one group head (monitoring node).

4.2 Group Formation

In this paper, an algorithm is proposed where intrusion detection has been done in a group based manner to take care of the wormhole attacks. The AODV routing protocol is used as the underlying network topology. The group based approach is introduced to reduce the load of processing on each group heads. From security point of view, this will also reduce the risk of a group head being compromised.

The entire network is divided in group . The group may be overlapped or disjoint. Each group has its own group head and a number of nodes designated as member nodes. Member nodes pass on the information only to the group head. The group head is responsible for passing on the aggregate information to all its members. The group head is elected dynamically and maintains the routing information.

W is the ward node, used for monitoring the malicious activity. The main purpose of the ward node is to save the group from possible attacks. The ward node has the power to monitor the activity of any node within the group. The ward node reports to the group head in case a malicious activity is detected. A group head detects a malicious activity.

4.3 Detection Technique Of Wormholes

Before, presenting the actual algorithm for detection of wormhole attacks, the data structure used for the purpose has been described below.

1. Threshold tolerance (P_{th}): This refers to the threshold value defined by the monitoring node. It is the tolerance value for lost packets.

2. Expected route trip time (T_e): Expected route trip time of a packet to a destination node is calculated as the time taken when the source node send HELLO packet to the destination node and get back an acknowledgement for that.

3. Route trip time (T_r): When the source node send packet it starts a timer. On receipt of an acknowledgement, the timer is stopped. The total time elapsed is recorded as Tr

4. P_s: Number of packets sent to a destination node D from source node S.

5. P_d: Number of packets received by node D from a specific source node S.

In figure 2 node S sends a HELLO message for destination node D. S has a path to D via (3). M1, being in the proximity of S, overhears the HELLO message and

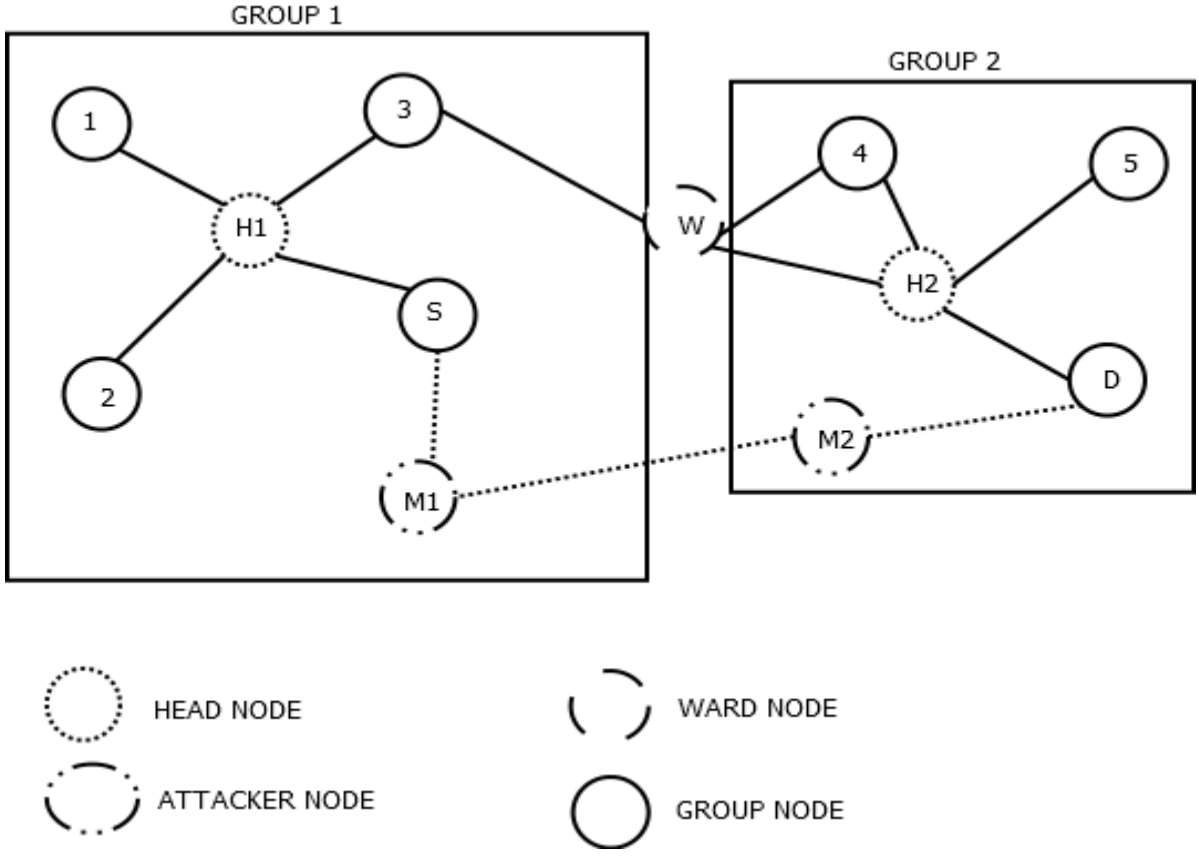

Figure 2: Group Based Detection Technique

forwards the same to node M2 in the other end of the network. Node D hears this HELLO message from S and therefore considers S to be its immediate neighbour and follow the route to send message to S via M1 and M2. The node w which is at the overlapping position of two group acts as ward node who can here every packet send by node S for the destination node D and monitor the packets route from source to destination. The ward node is also called monitoring node. When S observes some malicious behavior when it sends packet to D it informs the ward node. The ward node then checks the number of packets send for the node D and those actually received by D from S. Then it calculates $\Delta p = P_s - P_r$. If the value of Δp exceeds the threshold value P_{th} that is predefined by the monitoring node then monitoring node finds out the wormhole attack.

4.4 Procedure Of Wormhole Detection

Begin

Step-1 Initiate the network with two groups and each group have some nodes.

Step-2 The node within a group having minimum node id becomes group head. The node id for each node is provided when the node enter into the group.

Step-3 The node nearest to both the group head is chosen as the ward node.

Step-4 Source S sends hello message to the intermediate node with destination node id .

Step-4.1 Source S initialize timer at T_1.

Step-4.2 When destination receives packet it unicast the acknowledgement to the Source S.

Step-4.3 When acknowledgement receives by source S then it records time T_2.

Step-4.4 Now we calculate expected route trip time T_e as [$T_e = T_2 - T_1$].

Step-4.5 Source S sends packet to destination node and it records t1 at the time of sending the packet (at source) and then records t_2 at the time when source receives acknowledgement from the destination node.

Step-4.6 Now calculate route trip time as [$T_r = t_2 - t_1$].

Step-4.7 Now compare route trip time T_r with expected route trip time T_e and check for $T_r << T_e$.

Step-5 Then the ward node checks packets sent by source (P_s) and packets received by destination (P_r).

Step-6 Calculate [$\Delta p = P_s - P_r$] .

Step-7 Compare Δp which could be Drop with the threshold value $P_{th.}$.

Step-8 If ($\Delta p > P_{th}$) then inform the source node to stop packet transfer.

Step-9 The source node stop packet transfer inform group head.

End

5. CONCLUSION

In this paper, a new group based wormhole detection method has been proposed. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security threats including the wormhole attack. A number of recent works have been studied before proposing this new methodology. The proposed solution unlike some of its predecessors does not require any specialized hardware like directional antennas, etc for detecting the attackers or extremely accurate clocks, etc. Currently more studies are being done to analyze the performance of the proposed algorithm in presence of multiple attacker nodes.

6. ACKNOWLEDGEMENTS

This research paper is made possible through the help and support from everyone, including: parents, teachers, family and friends.

We would like to thank Mr. Sandeep Saxena and Mr. Aatif Jamshed for his support and encouragement and thank to our parents, family, and friends, who provide the advice and support. This research paper would not be possible without all of them.

7. REFERENCES

[1] Y. Hu, A. Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks, in Proc. of INFOCOM 2003, San Francisco, CA, USA, April 2003.

[2] Marko Jahnke, Jens Toelle, Alexander Finkenbrink,. Alexander Wenzel, et.al; "Methodologies and Frameworks for Testing IDS in ad-hoc Networks"; Proceedings of the 3rd ACM workshop on QOS and security for wireless and mobile networks; Chania, Crete Island, Greece, Pages: 113 - 122, 2007.

[3] Y.-C. Hu, A. Perrig, D. B. Johnson; "Wormhole Attacks in Wireless Networks"; IEEE Journal on Selected Areas of Communications, vol. 24, numb. 2, pp. 370-380, 2006.

[4] F.Hong, L. Hong, C. Fu; "Secure OLSR"; 19th International Conference on Advanced Information Networking and Applications, AINA 2005, Vol. 1, 25-30, pp. 713-718, March 2005[4] Y.-C. Hu, A. Perrig, D. B. Johnson; "Packet leashes: a defense against wormhole attacks in wireless networks"; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, pp. 1976-1986, 2003.

[5] Y.-C. Hu, A. Perrig; "A Survey of Secure Wireless Ad Hoc Routing"; Security and Privacy Magazine, IEEE, vol. 2, issue 3, pp. 28-39, May 2004.

[6] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing" in Proc. 2nd IEEE Workshop on Mobile Comput. Syst. Appl., Feb. 1999, pp. 90–100.

[7] Yang, H. and Luo, H. and Ye, F. and Lu, S. and Zhang, U.; "Security in Mobile Ad Hoc Networks: Challenges and Solutions"; Wireless Communications, IEEE, vol. 11, num. 1, pp. 38-47, 2004 .

[8] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop on Mobile Comput. Syst. Appl. routing," in Proc. 2nd IEEE Workshop on Mobile Comput. Syst. Appl.

[9] A. Mishra, K. Nadkarni, A. Patcha; "Intrusion Detection in Wireless Ad Hoc Networks"; IEEE Wireless Communications, Vol 11, issue 1, pg. 48-60, February 2004.

[10] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, L. Viennot; "Optimized Link State Routing Protocol"; Proceedings of IEEE INMIC, Pakistan 2001.

[11] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in Mobile Computing, T. Imielinski and H. Korth, Eds. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[12] D. B. Johnson, D. A. Maltz, and J. Broch, "The dynamic source routing protocol for multihop wireless ad hoc networks," in Ad-Hoc Networking. Reading, MA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[13] L. Hong, C. Fu; "Secure OLSR"; 19th International Conference on Advanced Information Networking and Applications, AINA 2005, Vol. 1, 25-30, pp. 713-718, March 2005.

[14] S. Capkun, L. Buttyan, J.-P. Hubaux; "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks"; Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks; 2003.

[15] Y-C Hu, A. Perrig, D. Johnson; "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols"; Proc. of WISE 2003, September 19, San Diego, California, USA, 2003.

[16] Korkmaz T.; "Verifying Physical Presence of Neighbours against Replay-based Attacks in Wireless Ad Hoc Networks"; Proc. International Conference on Information Technology: Coding and Computing 2005, ITCC 2005, pp. 704-709, 2005.