A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network

Moutushi Singh, Rupayan Das

Abstract— The nature of wireless ad hoc and sensor networks make them very attractive to attackers. One of the most popular and serious attack in wireless ad hoc and sensor network is the wormhole attack. It is a particularly severe attack on routing protocols for ad hoc networks in which two or more colluding attackers record packets at one location, and tunnel them to another location for a replay at that remote location. When this attack targets routing control packets, the nodes that are close to the attackers are defended from any alternative routes with more than one or two hops to the remote location. All routes are thus directed to the wormhole established by the attackers. This paper focuses on Wormhole attack detection in wireless sensor network. The wormhole attack is particularly challenging to deal with since the adversary does not need to compromise any nodes and can use laptops or other wireless devices to send the packets on a low latency channel. In This paper we have discussed and compared some of the very popular techniques for detecting this kind of attack.

Index Terms— Intrusion detection, Wormhole attack, QoS, jitter, delay, PSD, malicious node.

1 Introduction

Wireless Sensor networks are comprised of many small and resource constrained sensor nodes that are deployed in an environment for many applications which require unattended, long-term operations. In WSNs, each node serves as a router for other nodes, which allows data to travel by utilizing multi-hop network paths without relying on wired infrastructure. Due to numerous constraints such as, lack of infrastructure, dynamic topology and lack of pre-established trust relationships between nodes, most of the envisioned routing protocols for ad hoc networks are vulnerable to a number of solve challenging real world problems which continues to attract attention from industrial and academic research environment. Applications are emerging and widespread adoption is on the horizon. Most previous ad hoc networking research issues has focused on problems like routing and communication in a trusted environment. However, many applications run in untrusted environments and require secure communication and routing. Applications that requires secure communications like emergency response operations, military or police networks and safety-critical business operations such as oil drilling platforms or mining operations. For example, in emergency response operations such as after a natural calamity like a flood, tornado, hurricane, or earthquake, ad hoc networks could be used for real-time safety feedback. Here regular communication networks may be damaged, so emergency rescue teams nowadays rely upon ad hoc networks for better communication [2].

The remainder of this paper is organized as follows. In section 2 we present the concept of Intrusion Detection. In section 3 we present the basics of Wormhole Attack. In section 4 different literatures are surveyed on the techniques of wormhole attack detection and prevention. In section 5 comparison of the techniques are done based on their features. Finally conclusion is given in section 6.

2 Intrusion detection

An intrusion detection system (IDS) inspects all inbound and outbound network activities and identifies suspicious patterns that may indicate a network or system attack from an attacker attempting to break into or conciliation a system. With the wide spread use of computer networks the number of attacks has grown extensively and many new hacking tools and intrusive methods have appeared. Using an Intrusion Detection System (IDS) is one way of dealing with suspicious activities within a network.This System monitors the activities of a given environment and decides whether these activities are malicious (Intrusive) or genuine (normal) based on system integrity, confidentiality and the availability of information resources. The Intrusion Detection System collects information about the system being observed. This collected audit data is processed by the detector. The detector eliminates unnecessary information from the audit data and then makes a decision to evaluate the probability that these activities can be considered as a sign of an intrusion [1] [3].

There are following five measures to evaluate the efficiency of an intrusion detection system. They are:

Accuracy – incorrectness occurs when an intrusion detection system flags as abnormal or intrusive a genuine action in the surroundings.

Performance – The performance of an intrusion detection system is the rate at which audit events are processed. If the performance of the intrusion detection is deprived, then real-time detection is not possible.

Completeness – Incompleteness occurs when the intrusion detection system fails to detect an attack. This measure is very difficult to assess because it is impossible to have a global knowledge about the attacks or abuses of privileges.

Fault Tolerance – An intrusion detection system should itself be dead set against to attacks, especially denial of service. This is very important because most of the intrusion detection systems run on top of commercially available operating systems or hardware, which are known to be susceptible to attacks.

Timeliness – An intrusion detection system has to perform and propagate its analysis as quickly as possible to enable security events. This implies more than the measure of performance, because it not only encompasses the essential processing speed of theintrusion detection system, but also the time required to transmit the same and to reply to it.

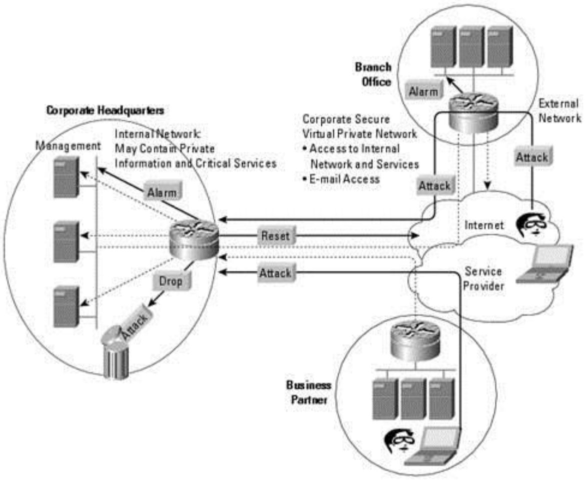

Fig. 1 Intrusion Detection System for Security Management

3 Wormhole attack

A wormhole attack is considered dangerous as it is independent of MAC layer protocols and immune to cryptographic techniques. In wormhole attacks, attackers create a low-latency link between two points in the network. This can be achieved by either compromising two or more sensor nodes of the network or adding a new set of malicious nodes to the network. Two attackers connected by a High speed Off-channel Link, are strategically placed at different ends of a network. Once the link is established, the attacker collects data packets on one end of the link, sends the data packets using the low-latency link and replays them at the other end [4].

Here X & Y be two Wormholes (Intruder) connected by Wormhole link.X replays in its neighbourhood (in area A) everything that Y hears in its own neighbourhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbors and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through them and use the large amount of collected information to break any network security.

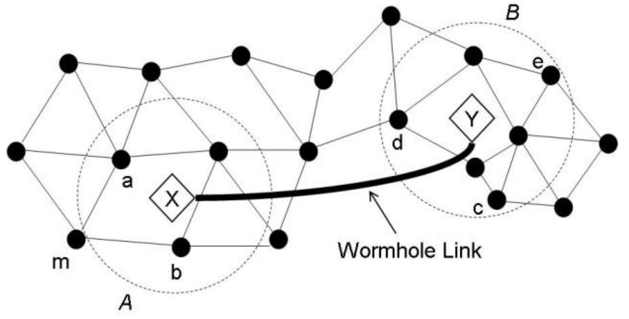

Fig. 2 Wormhole attack

In a wormhole attack using wired links or a high quality wireless out-of-band links, attackers are directly linked to each other, so they can communicate swiftly. However they need special hardware to support such communication. On the contrarily, a wormhole using packet encapsulation is relatively much slower, but it can be launched easily since it does not need any special hardware or special routing protocols [1] [2] [4].

There are two types of wormhole attack: Hidden Mode (HM) and Participation Mode (PM). HM wormhole nodes are concealed from genuine nodes as they do not process routing packets. They simply capture, tunnel and forward packets to each other and never appear in routing tables. Distinctively, PM wormhole nodes are visible during the routing process since they process routing packets as any normal node.

Significance of Wormhole Attack

Though wormhole is a useful networking service because it simply presents a long network link to the link layer and up, the attacker may use this link for his own benefit. After the attacker attracts a lot of data traffic through the wormhole, it can interrupt the data flow by selectively sinking or modifying data packets, generating gratuitous routing activities by turning off the wormhole link sporadically [4]. The attacker can also simply record the traffic for later analysis. Using wormholes an attacker can also break any protocol that directly or indirectly relies on geographic immediacy. Like, target tracking applications in sensor networks can be easily mystified in the presence of wormholes. Likewise, wormholes will affect connectivity-based localization algorithms, as two neighboring nodes are localized in close proximity and the wormhole links essentially ‘fold’ the entire network. This can have a major impact as location is a useful service in many protocols and application, and often out-of-band location systems such as

GPS are considered expensive or unusable because of the environment [5].

4 Literature Survey

In this paper several wormhole detection and prevention techniques are discussed. All the techniques are having their own advantages ans disadvantages.

The authors of [6] have discussed about localization-based systems, which are susceptible to wormhole attacks as they can disturb the localization procedure. For preventing the effect of wormhole attack, a 'distance-consistency-based secure location' scheme was projected, which incorporated wormhole attack detection, valid location recognition and self-localization. To achieve secure localization in the network and shielding against wormhole attack, Chen et al. [7]make a 'conflicting-set' for each node to use all differing sets of its adjacent locators for filtering out incorrect distance measurements of its adjacent locators. But the downside of this method is that it only works properly when the system has no packet loss. As the attackers may drop the packets intentionally, the packet loss is unavoidable when the system is underneath a wormhole attack.

In case of Localization based approach, Lazos and Poovendran [8] developed a "graph-theoretical" approach for the prevention of wormhole attack. The anticipated protocol is based on the use of limited location-aware guard nodes (LAGNs) which are in the known location and initiation and achieved through GPS receivers. LAGNs use "local broadcast keys" that are valid only between instant one hop neighbors. In their proposed protocol, for challenging wormhole attackers, a message encrypted with a local key - encrypted with the pair-wise key - at one end of the network and will not be decrypted at the other end. In [8] it is recommended that, use of hashed messages from LAGNs to sense wormholes during the key founding. A node can detect certain inconsistencies in messages from different LAGNs if a wormhole is present. In the absence of wormhole, a node is not capable to have the sense of hearing two LAGNs that are away, and are not able to hear the same message from one protector twofold.

The authors of [9] proposed the Hop Count (delay per hop indication [DELPHI] method. Both the hop count and delay per hop indication (DelPHI) are monitored for wormhole detection here. The elementary assumption in [9] is that, the rescheduling of a packet under normal condition for propagating one hop is very high in wormhole attack as the actual path between the nodes is longer than the advertised path. Like[9], the proposed methodology in [10] for wormhole detection is also a two-step process. In the first phase, from a set of dislodge paths from sender to receiver, the route path information are collected. Each sender embraces a timestamp on a special DREQ packet and sign it before sending it to the receiver. Each node upon receiving the packet for first time will include its node ID and increase the hop count by 1 and discards the packet next time onwards. The DREP packets will be sent by the receiver for each dislodge path received by it. For three times this course of action is carried out and the shortest delay and hop count information is selected for wormhole detection. In the second phase, the round trip time (RTT) is taken by calculating the time discrepancy between the packet it had sent to its neighbor and the reply received by it. The delay per hop value (DPH) is calculated as RTT/2h, where h is the hop count to the particular neighbor. A smaller h will have smaller RTT in normal conditions.But, under wormhole attack, a smaller hop count is having a larger RTT. If one DPH value for node X exceeds the consecutive one by some threshold, then the path through node X to all other paths with DPH values larger than it is treated as under wormhole attack[10] [11] . The authors of [12] proposed another technique for the detection of Wormhole attack, which is Hello Message timing interval procedure. Here revealing of wormhole nodes is done due to the Hello control messages. As a metric of compliance with the Optimized Link State Routing (OLSR) protocol, the percentage of HELLO Message Timing Intervals (HMTIs) that fall within a range is surrounded by the amount of jitter. A range R = [T - δ, T + δ] is defined. If an HMTI is in this range R, it is considered to be legitimate; otherwise it is out-of-protocol. An inferior test is done whenever the Hello Message Timing Interval packet behavior is doubtful. On the contrarary , a weakly performing node is associated with it a relatively large number of retry packets, which would not be the case with an attacking node. In this way, the problem of false positive alarms is solved[11] [12].

In case of both SAW [13] & DAW [14] technique, similar methodologies are discussed. But the major difference is the use of routing protocols. In reference [13], AODV protocol was followed while in [14], DSR routing protocol was used [17] [18]. In both of these papers, trust based security models have been proposed and used to detect intrusion. Arithmetical methods are used to identify the wormhole attack. If any link is found to be doubtful, then existing trust information is used to identify the wormhole tunnel. In this trust model , nodes observe neighbors based on the pattern of their packet drop but not on the number of packet drops. In [14], another algorithm for detecting the presence of wormhole WSN is proposed. Here, after sending the RREQ, the source waits for the RREP. The source receives many RREP coming through different routes. The link with very high frequency is checked and the value is checked with a previously defined threshold coefficient value. If the number of packet drop is higher than the number of packets sent, then there is the presence of wormhole.

The Cluster based detection technique is used in [15]. The authors of [15] have made an assumption that the MANET is made of a cluster of nodes. The underlying routing topology is AODV [16] [17].Different data structures are described to understand and propose the algorithm. Two layers have been described. When a node in the cluster of layer 1 expect wormhole attack within the cluster, it informs the cluster head of layer 1, which informs the cluster head at layer 2 about the malicious node. This cluster head of layer 2, broadcasts this information to all the cluster heads at layer 1. The cluster heads at layer 1 then inform their respective cluster members within the cluster.

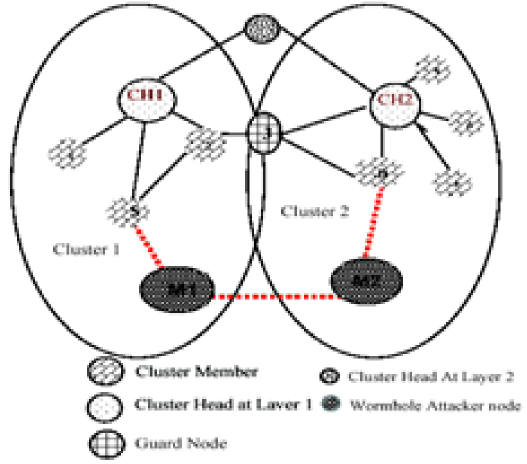

Fig. 3 Cluster Based Detection Technique

In Fig. 3, source node S sends a HELLO packet to destination node D. S has a path to D via (2, 3). M1, being in the closeness of S, overhears the HELLO message and forwards the same to node M2 in the other cluster of the network. Node D hears this HELLO message from S and therefore considers S to be its immediate neighbor and follow the route to send message to S via M1 and M2. The node 3 which is at the overlapping position of two cluster acts as GUARD 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 guard node is also called monitoring node. When S observes some malicious behavior when it sends packet to D it informs the guard node. The guard node then checks the number of packets send for the node D and those actually received by D from S. Then it calculates Δp = PKTSNT(S, D) - PKTRCD (S, D). If the value of Δp surmounts the threshold value that is predefined by the monitoring node then monitoring node finds out the wormhole attack [15].

He Ronghui et. Al. in [19] have described wormhole attack detection in wireless sensor networks with the use of Beacon nodes.This paper introduces an easy and effective method to detect and locate the wormholes. As wormhole attack is reactive, it happens only when a message is being transmitted in the area near a wormhole. A distributed algorithm is used to detect and locate a wormhole attack, in which each beacon node acts as a detector, each sensor node participates for hop counting, while the base station controls the start and end of the detecting procedure, and estimates the locations of wormhole ends based on alarm messages sent from beacon nodes. It acts like the Guard nodes of Cluster based technique [15]. This paper presents a distributed wormhole detection and localization algorithm which takes advantage of the known locations of beacon nodes. Its calculation cost is very low compared to those extra hardwares such as directional antennas and accurate clocks or manual setup of networks. It also provides the location of wormhole with a very small localization error.

In [20], the authors described the End to End Detection of Wormhole Attack (EDWA) technique. In some routing protocols of wireless ad hoc networks like AODV [17] and DSR [18], the source node first initiates a routing discovery by broadcasting a ROUTE REQUEST packet. All intermediate nodes continue broadcasting the ROUTE REQUEST upon receiving it until the ROUTE REQUEST reaches the destination or some nodes that have a route to the destination. Then a ROUTE REPLY will be unicasted back to the source along a routing table or according to the path in the packet header. The authors have modified these routing protocols to make them flexible with the wormhole attack. After sending the packet, it retrieves the receiver's site from the packet. Based on measurement of the sites, the sender estimates the shortest path in terms of hop count. The sender also retrieves the hop count value from the received ROUTE REPLY packet and compares it with the estimated value. We denote the estimated hop count of the shortest path as he and the value from the ROUTE REPLY packet as hr. If the received hop count value is smaller than the estimation, that is hr < _he, the sender predicts a wormhole attack and will mark the corresponding route. Once a wormhole is detected by the sender, the sender temporarily enables the path with wormhole and sends out a TRACING packet to the receiver. This TRACING packet is forwarded by each midway node through the route with wormhole. When a node in the route receives the TRACING packet, it acknowledges the source node with its current position by replying a TRACING-RESPONSE packet. The source will then estimate shortest path to each midway node and identify the two end points of the wormhole in a small area. An ERROR message is broadcasted to inform the presence of wormhole.

A new scheme called Statistical Analysis of Multi-path (SAM) is proposed in [21]. The authors used the maximum probability of relative frequency of a link to occur in the set of all obtained routes from one route discovery and the difference between the most frequently appeared link and the second most frequently appeared links in the set of all obtained routes from one route discovery, which will be higher in the presence of wormhole attack. The probability mass function (PMF) is used to get that the maximum relative frequency, which is more for a system under wormhole attack as compared to a normal system.

The authors of [22] used a trust based model for the identification of wormhole in the sensor network. In trust-based systems, each source node uses its trust information to calculate the most reliable path to a particular destination by circumventing intermediary malicious nodes. A wormhole in a system have the least trust level if that wormhole drops all the packets and if all the packets sent reach the destination then the neighboring node of a source node will have the highest trust level.

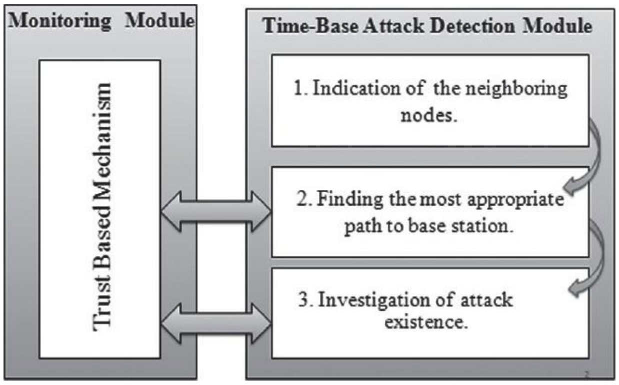
Monitoring Module
Trust Based Mechanism
Time-Base Attack Detection Module
1. Indication of the neighboring nodes.
2. Finding the most appropriate path to base station.
3. Investigation of attack existence.

Fig. 4 Time and Trust Based Detection Technique

It is a combined time and trust based model which detects the compromised nodes for false detection. These two models run together. Malicious nodes on the path can give the wrong impression about the time-based module by providing incorrect information. To prevent this problem, trust-based module always observes the first module and calculates trust values of neighbor nodes. These values are used to modify the path next time.

5 Comparison of Different Techniques of detecting Wormhole Attack

Since wormhole attacks are easy to implement but hard to detect, wormhole prevention and detection has been an attractive research problem. Here we have surveyed various wormhole detection techniques and tried to find out their features.

6 Conclusion

Wormhole attacks in WSNs can significantly degrade network performance and threaten network security. In wormhole attacks, as adversaries usually replay the genuine data packets, detection of these attacks is quite complicated. In this paper we have discussed what wormhole attack is actually and how to detect them in wireless environment. All the detection procedures have their own benefits and drawbacks. But there is no detection procedure which detects wormhole attack perfectly. Here we have basically surveyed the existing approaches which will help us in future to design a new approach for detecting the wormhole attack in wireless sensor network and MANET.

TABLE 1
Comparison of The Techniques

Techniques	Advantages	Disadvantages
Localized algorithm	Two Conflicting sets of each node filter out incorrect distance measurements.	Works only incase of no packet loss which is unavoidable when the system is under wormhole attack
Graph Theoretical Approach	Use of encryption techniques	Guard node uses local broadcast keys which are available only in one hop neighbors.
DELPHI	1. Both delay & hop count is measured 2. Synchronization is not required	1. Rescheduling of a packet propagating one hop is very high. 2. False alarm is not detected.
HMTI	1. False positive alarm problem is solved. 2. Synchronization is not required	Jitter is to be calculated. This jitter surrounds the HMTI.
SAW & DAW	Arithmetical Trust based security model is used.	Failed to detect false alarm detection.
Cluster based	1. Guard nodes are used to inform cluster heads about the attack. 2. No special hardwires are used.	It is only applicable for layered architecture of the network.
Beacon node	1. Beacon nodes are used & their location is known. 2. Calculation cost is low. 3. It provides very low localization error.	It is only applicable for layered architecture of the network.
EDWA	Shortest path is identified	Always the routing table & the packet header are checked for Request-Reply procedure.
SAM	Probability Mass function is used for identifying Wormhole Attack	If any real neighbor connection is wrongly labeled as wormhole false positive alarm will be caused
Trust Based Model	Trust values are used for modification of the path next time	This system is robust only when time and trust based modules are combined together

REFERENCES

[1] Farid Na¨ýt-Abdesselam, Brahim Bensaou and Tarik Taleb "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks" University of Sciences and Technologies of Lille, France.

[2] Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE," Wormhole Attacks in Wireless Networks", IEEE Journal on selected areas in Communications, vol. 24, no. 2, February 2006

[3] G. Mohammed Nazer, A. Arul Lawrence Selvakumar, "Current Intrusion Detection Techniques in Information Technology - A Detailed Analysis", European Journal of Scientific Research ISSN 1450-216X Vol.65 No.4 (2011), pp. 611-624

[4] Ritesh Maheshwari, Jie Gao and Samir R Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", Department of Computer Science, Stony Brook University Stony Brook, NY 11794-4400, USA

[5] Marianne Azer et al. ," A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009

[6] H. Chen, W. Lou, X. Sun, and Z. Wang. "A secure localization approach against wormhole attacks using distance consistency," EURASIP Journal on Wireless Communication and Networking- Special Issue on Wireless Network Algorithms, Systems, and Applications, pp. 22−32, 2010.

[7] H. Chen, W. Lou, and Z. Wang. "Conflicting-set-based wormhole attack resistant localization in wireless sensor networks," Book Chapter Lecture Notes in Computer Science − Ubiquitous Intelligence and Computing, vol. 5585/2009, pp. 296−309, 2009.

[8] L. Lazos and R. Poovendran, "Serloc: Secure range-independent localization for wireless sensor networks," Proceedings of the ACM Workshop on Wireless Security, pp. 21−30, Oct. 2004.

[9] H.S. Chiu and K. Lui. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks". In Proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, 2006.

[10] F. Nait-Abdesselam, B. Bensaou, T. Taleb. "Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks", IEEE Communications Magazine, 46 (4), pp. 127 - 133, 2008

[11] Reshmi Maulik and Nabendu Chaki, " A Study of Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279

[12] M.A. Gorlatova, P.C. Mason, M. Wang, L. Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis". In IEEE Military Communications Conference, pp. 1-7, 200

[13] M.S. Sankaran, S. Poddar, P.S. Das, S. Selvakumar. "A Novel Security model SaW: Security against Wormhole attack in Wireless Sensor Networks". In Proceedings of International Conference on PDCN, 2009

[14] Khin Sandar Win. "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology, 48, pp. 422-428, 2008

[15] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki," A New Cluster-based Wormhole Intrusion Detection algorithm for Mobile Ad-hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009

[16] Chaki, Rituparna; Chaki, Nabendu; "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network"; Proc. of the 6th Int'l Conf. on Computer Information Systems and Industrial Management Applications (CISIM '07); pp. 179 - 184, June 2007; ISBN: 0-7695-2894-5

[17] C.E perkins ,E.M Royer and SR Das." Ad-hoc on demand distance vector routing", the 2nd IEEE workshop on mobile computing system and application pages 90-100, Feb. 1999.

[18] D. B. Johnson, D. A. Maltz, and Y. Hu," The dynamic source routing protocol for mobile ad hoc networks (DSR)", IET-FMANET Internet Draft, 2003.

[19] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan, "Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes", World Academy of Science, Engineering and Technology 55 2009.

[20] Xia Wang, JohnnyWong," An End-to-end Detection ofWormhole Attack in Wireless Ad-hoc Networks", Department of Computer Science Iowa State University Ames, Iowa 50011

[21] N. Song, L. Qian, X. Li. "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach". In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, pp. 8-15, 2005.

[22] 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