Survey Detection and Prevention Scheme against Wormhole Attack in MANET

Mohini Gupta, Amit Kanungo

Abstract— In Mobile ad hoc network (MANET) various routing attacks for single-path routing have been proposed in previous work. These nodes communicate with each other by interchange of packets, which for those nodes not in wireless range goes hop by hop. Due to absence of a defined central authority, securing the routing process becomes a challenging task thereby leaving MANETs vulnerable to attacks, by that the deterioration in the performance characteristics as well as raises a serious question mark about the reliability of such networks. This last point is where the main problem for MANET security resides, the ad hoc networks can be reached very easily by users, but also by malicious attackers. If a malicious attacker reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network. In this paper we presents the overview of types of attacks and their solution to recognizes the effect of attacker and security schemes.

Keywords:- MANET, Routing, Attack, survey, Security scheme.

I. INTRODUCTION

Mobile ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. They usually have a dynamic topology such that nodes can easily join or leave the network at any time and they move around freely which gives them the name Mobile Ad hoc Networks or MANETs. They have many potential applications, especially in military and rescue operations such as connecting soldiers in the battle field or establishing a temporary network in place of one which collapsed after a disaster like an earthquake.

In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. Figure 1.1 represents the mobile ad hoc network.

To support connectivity nodes are uses routing protocols such as AODV [1] (Ad hoc On Demand Distance Vector Routing Protocol). Mobile ad-hoc networks are usually susceptible to different security threats and malicious node attack is one of these. In this attack, a attacker nodes which absorbs and drops all data packets makes use of the vulnerabilities of the on demand route discovery protocols. According to the routing strategy routing protocols can be classified as Table-driven or Proactive routing protocols and on demand or source initiated.

Manuscript received June 2013

Miss. Mohini Gupta, (M.Tech. Scholar) Medicaps Institute of Technology & Management Indore (M.P.) India.

Prof. Amit Kanungo, Medicaps Institute of Technology & Management Indore (M.P.) India.

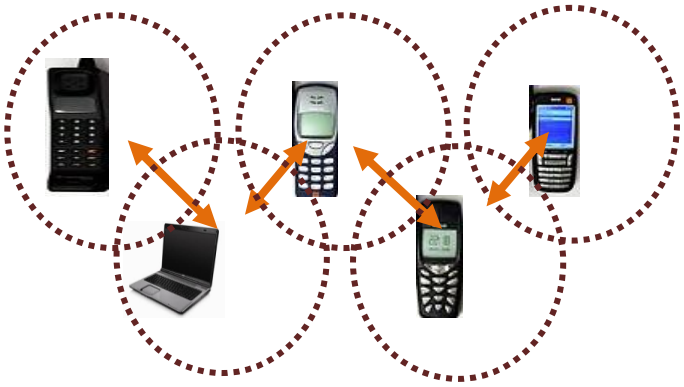

Fig.1. Ad hoc Network

Mobile ad hoc networks originated from the U.S. Government's Defence Advanced Research Projects Agency (DARPA) Packet Radio Network (PRNet) and SURAN project. Being independent on re-established infrastructure, mobile ad hoc networks have advantages such as rapidity and ease of deployment, improved flexibility, and reduced costs. Mobile ad hoc networks are appropriate for mobile applications in either hostile environment where no infrastructure is available, or temporarily established mobile applications, which are cost crucial.

II. ROUTING IN MANET

It has become clear that routing in a MANET is fundamentally different from traditional routing found on infrastructure networks. Routing in a MANET depends on many factors including topology, selection of routers, and initiation of request and specific underlying characteristic that could serve as a heuristic in finding the path quickly and efficiently. The low resource availability in these networks demands efficient utilization and hence the motivation for optimal routing in ad hoc networks. Also, the highly dynamic nature of these networks imposes severe restrictions on routing protocols specifically designed for them, thus motivating the study of protocols which aim at achieving routing stability.

III. CLASSIFICATION OF ROUTING PROTOCOLS IN MANET

The routing protocols in MANET are classified depending on routing strategy and network structure. According to the routing strategy the routing protocols can be categorized as Table-driven and source initiated, while depending on the

network structure these are classified as flat routing, hierarchical routing and geographic position assisted routing Based on the routing strategy the routing protocols can be classified into two parts:

3.1 Proactive, Reactive, and Hybrid Routing

One of the most popular methods to distinguish mobile ad hoc network routing protocols is based on how routing information is acquired and maintained by mobile nodes. Using this method, mobile ad hoc network routing protocols can be divided, as discussed above, into proactive routing, reactive routing, and hybrid routing.

A proactive routing protocol is also called a "table-driven" routing protocol. Using a proactive routing protocol, nodes in a mobile ad hoc network continuously evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. Therefore, a source node can get a routing path immediately if it needs one.

In proactive routing protocols, all nodes need to maintain a consistent view of the network topology. When a network topology change occurs, respective updates must be propagated throughout the network to notify the change. Most proactive routing protocols proposed for mobile ad hoc networks have inherited properties from algorithms used in wired networks. To adapt to the dynamic features of mobile ad hoc networks, necessary modifications have been made on traditional wired network routing protocols. Using proactive routing algorithms, mobile nodes proactively update the network state and maintain a route regardless of whether data traffic exists or not, and the overhead to maintain up-to-date network topology information is high. The next section will introduce several typical proactive mobile ad hoc network routing protocols, such as the WRP, DSDV, and the Fisheye State Routing (FSR) Protocols.

Reactive routing protocols for mobile ad hoc networks are also called "on-demand" routing protocols. In a reactive routing protocol, routing paths are searched only when needed. A route discovery operation invokes a route-determination procedure. The discovery procedure terminates when either a route has been found or no route is available after examination for all route permutations.

In a mobile ad hoc network, active routes may be disconnected due to node mobility. Therefore, route maintenance is an important operation of reactive routing protocols.Compared to the proactive routing protocols for mobile ad-hoc networks, less control overhead is a distinct advantage of the reactive routing protocols.

Thus, reactive routing protocols have better scalability than proactive routing protocols in mobile ad hoc networks. However, when using reactive routing protocols, source nodes may suffer from long delays for route searching before they can forward data packets. The Dynamic Source Routing (DSR) Protocol and Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol are examples of reactive routing protocols for mobile ad hoc networks.

Hybrid routing protocols are proposed to combine the merits of both proactive and reactive routing protocols and overcome their shortcomings. Normally, hybrid routing protocols for mobile ad hoc networks exploit hierarchical network architectures. The proper proactive routing approach and reactive routing approach are exploited in different hierarchical levels, respectively. In this chapter, as examples of hybrid routing protocols for mobile ad hoc networks, the Zone Routing Protocol (ZRP), Zone-Based Hierarchical Link State (ZHLS) Routing Protocol, and Hybrid Ad Hoc Routing Protocol (HARP) will be introduced and discussed.

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types.

IV. TYPES OF ATTACKS FACED BY ROUTING PROTOCOLS

Due to their underlined architecture, ad-hoc networks are more easily attacked than a wired network. The attacks prevalent on ad-hoc routing protocols can be broadly classified into passive and active attacks.

1. **Passive Attack**
   A Passive Attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks.
2. **Active Attack**
   An *Active Attack*, however, injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The goal is basically to attract all packets to the attacker for analysis or to disable the network. Such attacks can be detected and the nodes can be identified.

We will now present a brief overview of 3 of the more prominent attacks prevalent against ad-hoc networks, most of which are active attacks [5].

1) Attacks based on modification

This is the simplest way for a malicious node to disturb the operations of an ad-hoc network. The only task the malicious node needs to perform, is to announce better routes (to reach other nodes or just a specific one) than the ones presently existing. This kind of attack is based on the modification of the metric value for a route or by altering control message fields. There are 3 ways in which this can be achieved:

2) Redirection by Changing the Route Sequence Number: When deciding upon the best / optimum path to take through a network, the node always relies on a metric of values, such as hop count delays etc. the smaller that value, the more optimum the path. Hence, a simple way to attack a network is to change this value with a smaller number than the last "better" value.

3) Redirection by Altering the Hop Count: This attack is more specific to the AODV protocol wherein the optimum path is chosen by the hop count metric. A malicious node can disturb the network by announcing the smallest hop count value to reach the compromised node. In general, an attacker would use a value zero to ensure to the smallest hop count.

Taking for example the 'wormhole' attack,[14] an attacker records packets at one location in the network, tunnels them to another location, and retransmits them there into the network. This could potentially lead to a situation where, it would not be possible to find routes longer than one or two hops, probably disrupting communication.

4) Denial of Service by Altering Routing Information: Consider, in a bus topology, a scenario wherein a node A wants to communicate with node E. At node A the routing path in the header would be A-B-C-D-E. If B is a compromised node, it can alter this routing detail to A-B-C-E. But since there exists no direct route from C to E, C will drop the packet. Thus, A will never be able to access any service / information from E.

Another instance can be seen when considering a category of attacks called 'The Black Hole Attacks'. Here, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. Once the malicious node has been able to insert itself between the communicating nodes, it can do anything with the packets passing between them. It can then choose to drop the packets thereby creating a DoS.

5) Impersonation Attacks

More generally known as '*spoofing*', since the malicious node hides its' IP and or MAC address and uses that of another node. Since current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. Take for example a situation wherein an attacker creates loops in the network to isolate a node from the remainder of the network. To do this, the attacker needs to spoof the IP address of the node he wants to isolate from the network and then announce new route to the others nodes. By doing this, he can easily modify the network topology as he wants.

6) Attack by Fabrication of Information

There are basically 3 sub categories for fabrication attacks. In any of the 3 cases, detection is very difficult.

a. **Falsification of Rote Error Messages:** This attack is very prominent in AODV and DSR, because these two protocols use path maintenance to recover the optimum path when nodes move. The weakness of this architecture is that whenever a node moves, the closest node sends an "error" message to the other nodes so as to inform them that a route is no longer accessible. If an attacker can cause a DoS attack by spoofing any node and sending error messages to the all other nodes. Thus, the malicious node can isolate any node quite easily.

b. **Corrupting Routing State (Route Cache Poisoning):** A passive attack that can occur especially in DSR due to the promiscuous mode of updating routing tables which is employed. This occurs when information stored in routing tables is deleted, altered or injected with false information. A node overhearing any packet may add the routing information contained in that packet's header to its own route cache, even if that node is not on the path from source to destination. The vulnerability of this system is that an attacker could easily exploit this method of learning routes and poison route caches by broadcast a message with a spoofed IP address to other nodes. When they receive this message, the nodes would add this new route to their cache and would now communicate using the route to reach the malicious node.

c. **Routing table overflow attack:** Consider ad-hoc network is using a "proactive" protocol i.e. an algorithm which tries to find routing information even before it is needed. This creates vulnerabilities since the attacker can attempt to create routes to non-existent nodes. If enough routes are created, new routes can no longer be added due to an overwhelming pressure on the protocol.

After considering all the above plausible attacks we can draw a conclusion that we need to have a routing protocol that establishes routes without being susceptible to false information from any malicious node. A good routing protocol should also be able to detect the malicious nodes and to react in consequence, by changing routes, etc.

7) Worm hole

In a wormhole attack, 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 by that all packets are forwarded through tunnel and actual destination only wait for data.

8) Collusion attack. In collusion attack, some of the malicious nodes collude with each other and manipulate routing information of one or a number of other nodes such that those nodes will not be accessible in the network anymore [1], [4].

9) Black hole Attack. In Black hole attack, attacker node propagates unreal information in the network and tries to direct network traffic towards itself. Traffic absorption would be possible through suggesting optimized fake routes to other nodes of the network. Therefore, a considerable amount of network traffic would be absorbed by attacker node. Afterwards, Black hole node can misuse received information or discard them silently [1], [4], [8], [12].

10) Gray hole attack. Gray hole attack is a special form of Black hole in which after absorbing the network traffic, in some cases attacker node behaves like the other trusty nodes and forwards packets according to the routing algorithm; whereas in other cases, it drops received packets [8].

V. RELATED WORK

We are doing a work on attacks mentioned [2], a cluster based counter-measure for the wormhole attack alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET. Simulation results on MATLab exhibit the effectiveness of the proposed algorithm in detecting wormhole attacks. A two layer approach is used for detecting whether a node is participating in a wormhole attack. The layered approach is introduced to reduce the load of processing on each cluster heads. From security point of

view, this will also reduce the risk of a cluster head being compromised.

Choi et al. in [3] considered that all the nodes will monitor the behavior of its neighbors. Each node will send RREQ messages to destination by using its neighbor list. If the source does not receive back the RREP message within a stipulated time, it detects the presence of wormhole and adds the route to its wormhole list. Each node maintains a neighbor node table which contains a RREQ sequence number, neighbor node ID, sending time and receiving time of the RREQ and count. Here the source node sets the Wormhole Prevention Timer (WPT) after sending RREQ packet and wait until it overhears its neighbor's retransmission.

In [4], a new protocol called Multi-path Hop-count Analysis (MHA) is introduced based on hop-count analysis to avoid wormhole attack. It is assumed that too low or too high hop-count is not healthy for the network. The novelty of the hop-count analysis in detecting wormholes is however questionable. Similar works have also been reported earlier. As an example, Djenouri et al. [5] may be considered.

In [6], wormholes are detected by considering the fact that wormhole attacks consists of relatively longer packet latency than the normal wireless propagation latency on a single hop. Since the route through wormhole seems to be shorter, many other multi-hop routes are also channeled to the wormhole leading to longer queuing delays in wormhole. The links with delays are considered to be suspicious links, since the delay may also occur due to congestion and intra-nodal processing.

In reference [7], both the hop count and delay per hop indication (DelPHI) are monitored for wormhole detection. The fundamental assumption in is once again that the delay a packet experiences under normal circumstances for propagating one hop will become very high under wormhole attack as the actual path between the nodes is longer than the advertised path.

Specific detection uses rule-match methods to justify whether monitored traffic have special attack features [8]. The rule-match approaches maintaining per flow state and matching packets to a pre-defined set of rules [9] has shown a certain good capability. However, rule-match approaches unlikely detect unknown DDoS attacks.

Lakhina et a1. [10] Made use of maximum and relative entropy and subspace to mine and analyse traffic anomalies. For previous unknown DDoS attacks, anomaly-based detection has higher accuracy than rule-match approach. Anomaly-based detection models the behaviour of normal traffic and then reports any anomalies. PCA, entropy and subspace methods have demonstrated accuracy and efficiency in detecting network-wide traffic behaviour anomalies.

Ringer gets a1. [11] Used PCA (principal Component Analysis) to analyse the origin-destination flow aggregation and entropy time series of traffic features. However, most of these network-wide anomaly detection and machine-learning approaches are performed offline. Thus, it is difficult for them to take timely preventive measures for DDoS attacks.

Wang et a1. [12] Proposed a behavioural-distance based anomaly detection mechanism. In order to real-timely detect and defence DDoS attacks, on-line detection techniques are now paid wide attention. Generally, on-line detection techniques are statistical approaches regarding traffic feature and behaviours. Consequently, computation, memory consumption and detection time are key concerns about on-line detection.

Incentive based approaches aims to promote positive behaviour to foster cooperation instead of relying on participants to report and punish misbehaving nodes. Zhang et al. [13] [14] have developed a distributed and cooperative intrusion detection system (IDS) where individual IDS agents are placed on each and every node. Each IDS agent runs independently, detects intrusion from local traces and initiates response.

The Delay per Hop Indicator (DelPHI) [15] proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to find every available disjoint route between a sender and a receiver. Then, the delay time and length of each route are calculated and the average delay time per hop along each route is computed. These values are used to identify wormhole. The route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both types of wormhole attack; however, it cannot pinpoint the location of a wormhole.

Hu and Evans developed a protocol using directional antennas to prevent wormhole attacks [16]. Directional antennas are able to detect the angle of arrival of a signal. In this protocol, two nodes communicate knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle (i.e. one from west and the other at east). This protocol fails only if the attacker strategically placed wormholes residing between two directional antennas.

Rouba El Kaissi et.al [17] obstacles impede the successful deployment of sensor networks. In addition to the limited resources issue, security is a major concern especially for applications such as home security monitoring, military, and battle field applications. This paper presents a defense mechanism against wormhole attacks in wireless sensor networks.

Y. C. Hu et.al.[18] have considered packet leashes – geographic and temporal. In geographic leashes, node location information is used to bound the distance a packet can traverse. Since wormhole attacks can affect localization, the location information must be obtained via an out-of-band mechanism such as GPS. Further, the "legal" distance a packet can traverse is not always easy to determine. In temporal leashes, extremely accurate globally synchronized clocks are used to bound the propagation time of packets that could be hard to obtain particularly in low-cost sensor hardware. Even when available, such timing analysis may not be able to detect cut-through or physical layer wormhole attacks.

In S. Capkun et.al.[19], an authenticated distance bounding technique called MAD is used. The approach is similar to packet leashes at a high level, but does not require location information or clock synchronization. But it still suffers from other limitations of the packet leashes technique.

Albers et al. [20] proposed a distributed and collaborative architecture of IDS by *using mobile agents*. A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS. Two types of data are exchanged among LIDS: security data (to obtain complementary information from collaborating nodes) and intrusion alerts (to inform others of locally detected intrusion). In order to analyze the possible intrusion, data must be obtained from what the LIDS detects on, along with

additional information from other nodes. Other LIDS might be run on different operating systems or use data from different activities such as system, application, or network activities, therefore, the format of this raw data might be different, which makes it hard for LIDS to analyze. However, such difficulties can be solved by using Simple Network Management Protocol (SNMP) data located in Management Information Base (MIBs) as an audit data source. Such a data source not only eliminates those difficulties, but also reduces the increase in using additional resources to collect audit data if an SNMP agent is already run on each node. For the methodology of detection, Local IDS Agent can use either anomaly or misuse detection. However, the combination of two mechanisms will offer the better model. Once the local intrusion is detected, the LIDS initiates a response and informs the other nodes in the network. Upon receiving an alert, the LIDS can protect itself against the intrusion.

Kachirski and Guha [21] proposed a multi-sensor intrusion detection system based on mobile agent technology. The system can be divided into three main modules, each of which represents a mobile agent with certain functionality, i.e.: monitoring, decision-making and initiating a response.

a. Monitoring agent: Two functions are carried out at this class of agent: network monitoring and host monitoring.

b. Action agent: Every node also hosts this action agent. The action agent can initiate a response, such as terminating the process or blocking the node from the network, if it meets intrusion activities where it lives.

c. Decision agent: The decision agent is run only on certain nodes, mostly at the nodes that run network monitoring agents. If the local detection agent cannot make a decision on its own due to insufficient evidence of an intrusion, it will report to this decision agent in order to investigate deeply on the suspected node Since nodes move arbitrarily across the network, a static hierarchy is not suitable for such dynamic network topology.

Sterne et al. [22] proposed a dynamic intrusion detection hierarchy that is potentially scalable to large networks use clustering. This method is similar with Kachirski and Guha [21], but it can be structured in more than two levels. Thus, nodes on first level are cluster heads, while nodes on the second level are *leaf nodes*. In this model, every node has the task to monitor, log, analyze, respond, and alert or report to cluster heads. The Cluster heads, in addition, must also perform:1) Data fusion/integration and data filtering, 2) Computations of intrusion, and 3) Security Management.

B.Sun [23] proposed Zone Based IDS (ZBIDS). In the system, the MANET is spitted into non overlapping zones (zone A to zone I). The nodes can be categorized into two ypes: the intra zone node and the inter-zone node (or a gateway node). Each node has an IDS agent run on it.

This agent is similar to the IDS agent proposed by Zhang and Lee. Others components on the system are data collection module and detection engine, local aggregation and correlation (LACE) and global aggregation and correlation (GACE). The data collection and the detection engine are responsible for collecting local audit data (for instance, system call activities, and system log files) and analyzing collected data for any sign of intrusion respectively. The remainder, LACE module is responsible for combining the results of these local detection engines and generating alerts if any abnormal behavior is detected. These alerts are broadcasted to other nodes within the same zone. However, for the GACE, its functionality depends on the type of the node. If the node is an intra-zone node, it only sends the generated alerts to the inter-zone nodes.

Thus, if the node is an inter-zone node, it receives alerts from other intra-zone nodes, aggregates and correlates those alerts with its own alerts, and then generates alarms. The intrusion response module is responsible for handling the alarms generated from the GACE.

VI. CONCLUSION & FUTURE WORK

In this paper we have discussed some important an comprehensive simulation for security in MANET. The study focuses on how performance of network will affected from different attacks in a network. The study here establishes the foundation for future work towards designing a mechanism to identify the nodes which are actively involved in any attack. Intrusion prevention alone is not sufficient to achieve security in a network, we have hereby presented a way to manage MANET security, by enhancing the existing secure protocols adding the component of extermination of communication of malicious nodes, not only in determining the route for sending packages. There are basically two approaches for dealing with malicious nodes. The first one gives a motivation for participating in the network function. The second approach detects and excludes misbehaving nodes. Most of the existing systems belong to the second type. These systems use extra services or specific algorithms to detect misbehaving nodes in MANET and exclude them from the routing path.

In our future scope of work, we would hold this approach in minimizing the performance of a network from worm hole attack. We simulated attack in the ad-hoc networks and find its affects. In our study, we used the AODV routing protocol. But the other various routing protocols could be simulated also.

REFERENCES

[1] Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF "A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks", Paper presented at the IEEE 19th International Conference on Advanced Information. Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005.

[2] 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.

[3] S. Choi, D. Kim, D. Lee, J. Jung. "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks". In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343-348, 2008.

[4] Shang-Ming Jen, Chi-Sung Laih, Wen-Chung Kuo. "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", 9 (6), pp. 5022-5039, 2009.

[5] D. Djenouri, O. Mahmoudi, D. Llewellyn-Jones, M. Merabti, "On Securing MANET Routing Protocol Against Control Packet Dropping". In IEEE International Conference on Pervasive Services, pp. 100-108, 2007.

[6] 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.

[7] 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.

[8] T. Peng, C. Leckie and R. Kotagiri, "Survey of network-based defense mechanisms countering the DoS and DDoS problems", ACM Comput. Surv. 39, April 2007.

[19] R. Sommer and V. Paxson, "Enhancing byte-level network intrusion detection signatures with context", CCS, 2003.

[10] X. Li, F. Bian, M. Crovella, C. Diot, R. Govindan, G. Iannaccone and A. Lakhina, "Detection and identification of network anomalies using sketch subspaces", IMC, 2006.
[11] H. Ringerg, A. Soule, J. Rexford and C. Diot, "Sensitivity of pc a for traffic anomaly detection", SIGMETRICS, 2007.
[12] Hemant Sengar, Xinyuan Wang, Haining Wang, Duminda Wijesekera and Sushil Jajodia, "Online Detection of Network Traffic Anomalies Using Behavioural Distance", IEEE IWQoS 2009, Charleston, July 2009.
[13] Huaizhi Li; Singhal, M.;, "A Secure Routing Protocol for Wireless Ad Hoc Networks," System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on , vol.9, no., pp. 225a, 04-07 Jan. 2006.
[14] Razak, S.A., Furnell, S., Clarke, N. Brooke, P. Mehrotra, Sharad. Zeng, Daniel, Chen, Hsinchun. Thuraisingham, Bhavani. "A Two-Tier Intrusion Detection System for Mobile Ad Hoc Networks—A Friend Approach", Lecture Notes In Computer Science, volume 3975, pp. 590-595, 2006, Springer.
[15] D. A. Maltz and D. B. Johnson and Y. Hu. The dynamic source routing protocol (DSR) for mobile ad hoc.
[16] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proceedings of the Network and Distributed System Security Symposium.
[17] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy,"Dawsen: a defense mechanism against wormhole attacks in wireless sensor networks", IN Second International Conference on Innovations in Information Technology (IIT'05).
[18] Y. C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in INFOCOM, 2003.
[19] S. Capkun, L. Buttyn, and J. P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," in 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), October 2003.
[20] P. Albers, O. Camp, et al. "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches". Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.
[21] O. Kachirski, R. Guha. "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks." Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE, 2003
[22] D. Sterne, P. Balasubramanyam, et al. "A General Cooperative Intrusion Detection Architecture for MANETs". In Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, 2005.
[23] B. Sun, K.Wu, and U. W. Pooch. "Alert Aggregation in Mobile Ad Hoc Networks". The 2003 ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, 2003