REVIEW OF LITERATURE

Brands and Chaum (1994) propose a three-way handshake which bounds the distance between a node and a verifier by measuring the round trip time between them. Our technique is able to detect wormholes with only a single message, and requires corrections for clock skew between the sender and receiver.

S. Marthi, T. J. Giuli, K. Lai and M. Baker (2000) proposed the “watchdog and pathrater” scheme that is used to detect & mitigate the effect of nodes that do not forward packets. These two techniques were added to the standard routing protocol DSR in adhoc networks. Watchdog determines misbehavior by copying packets to be forwarded into a buffer and monitoring the behavior of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not. If the packets that are snooped match with the observing node’s buffer, then they are discarded; whereas packets that stay in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified. The node responsible for forwarding the packet is then noted ass being suspicious. If the number of violations becomes greater than a certain predetermined threshold, the violating node is marked being malicious. Information about malicious nodes is passed to the Pathrater component of for inclusion in the path rating evaluation. Pathrater on an individual node works to rate all of the known nodes in a particular network with respect of their reliabilities. Ratings are made and updating from a particular node’s perspective. Nodes start with a neutral rating that is modified over time based on observed reliable or unreliable behavior during packet routing. Nodes that are observed by watchdog to have misbehaved are given an immediate rating of 100. This way Pathrater helps in finding the possible routes excluding the misbehaving nodes.
D. B. J., Yih-Chun Hu, Adrian Perrig (2002) proposed a secure on-demand routing protocol for ad-hoc networks named as ARIADNE which is based on DSR & TESLA. This protocol provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptography. It also requires clock synchronization, which we consider to be an unrealistic requirement for ad hoc networks.

S. Buchegger and J. Le Boudec (2002) proposed CONFIDANT (Cooperation of Nodes, Fairness In Dynamic Ad-Hc Networks) system is based on direct observations and on second-hand information from other nodes, and is updated according to a Bayesian estimation. CONFIDANT consists of Monitoring System, Reputation System, Trust Manager and Path Manager. Their tasks are divided into two sections: the process to handle its own observations and the process to handle reports from trusted nodes. It is based on distributed and cooperative architecture. Its nodes cooperate and share alarm messages with the other nodes in the wireless ad-hoc network that are in a node’s friend list. If a node is observed to behave in a cooperative fashion, then positive reputation is assigned to it, otherwise a negative reputation is assigned to it. The alarm messages are evaluated based on their trustworthiness using Bayesian estimations.

Michiardi and Molva, (2002) proposed the CORE system (A Collaborative Reputation Mechanism to enforce node cooperation in MANETs), which uses game theoretic analysis to model reputation. Members that have good reputation, because they helpfully contribute to the community life, can use the resources, while members with a bad reputation, because they refuse to cooperate, are gradually excluded from the community. In CORE[15], the term “subjective reputation” is used to represent the reputation calculated from direct observations’ using a weighted mean of the observations rating factors, giving more relevance to the past observations. It also used indirect reputation exchanges from other nodes to obtain a global reputation value.
The difference between COORE and CONFIDANT is that CCORE only allows positive reports to pass through, but CONFIDANT allows negative reports also. This means that CORE prevents false reports. Therefore, it prevents a DoS attack which CONFIDANT cannot do.

Alberts et al. 2002 proposed another distributed 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 type of data are exchanged among LIDS: security data (to obtain complimentary information from collaborating nodes) and intrusion alerts (to inform others of locally detection intrusion). In order to analyse the possible intrusions, data must obtained from what the LIDS detects on, along with additional information from other nodes. Once the local intrusion is detected, the LDIS initiates a response and informs the other nodes in the network. Upon receiving an alert, the LIDS can protect itself against the intrusion.

H. Deng, W. Li, and D. P. Agrawal (2002) discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source node get this information, it sends a RREQ to the next hop to verify that the target node (i.e. the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a Further Request, it sends a Further Reply which includes the check result to the source node. Based on information in Further Reply, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. Obviously, this increases the routing overhead and end-to-end delay. In addition, the intermediate node needs to send RREP message twice for a single route request.
Kachirski and Guha (2003) proposed a hierarchical 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: monitoring, decision-making and initiating a response. Monitoring agents perform the network monitoring and host monitoring. Host monitoring agents are present on every node. A distributed algorithm is used to dynamically divide the mobile network into clusters and assigning only a few nodes – cluster heads, to host sensors that monitor network packets and agents that make decisions. Action agent resides on all network nodes, which initiate a response, such as terminating the process or blocking the node from the network, if it meets intrusion activities where it lives. The decision agent is run on 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.

Y.-C. Hu, A. Perrig, and D. Johnson (2003) propose the concept of a packet leash as a general mechanism for detecting and preventing wormhole attacks. Furthermore, they categorize the leashes into geo-graphical leashes and temporal. A geographical leash verifies that the receiver of a packet is within a certain distance from the sender whilst according to temporal leash the packet has an upper bound on its lifetime which bounds the maximum traverse distance. The latter mechanism is similar to our approach with the critical difference that all nodes must have tightly synchronized clocks using appropriate hardware. Another difference is that our mechanism advocates the sender of the message as the one that decides if a suspected wormhole attack has occurred, and not the receiver as the authors proposes obviously, when the receiver is an adversary and consequently helps with the creation of the wormhole tunnel the temporal leash concept is not enough to defend against the malicious collaborative nodes.
Johnson DB (2004) proposed a modified DSR protocol to defend against wormhole nodes by adopting a multi-path routing method. A source node initiates route discovery, and the destination node, after receiving multiple paths, begins to calculate the proportion of each link between two nodes in the total paths. Due to wormhole node’s great ability to grab routing paths, if the occurrence of one link exceeds the threshold value, the two ends of this link may be wormhole nodes. The destination would first send a test data packet to verify if this link is abnormal, such as the packet being dropped. If it is confirmed that the two ends of this link are wormhole nodes, the destination would send a warning message to the neighbors of the malicious nodes, informing them not to process any messages from the malicious nodes. In this way, the malicious nodes would be isolated, and then quarantined.

Hu and Evans (2004) propose to use directional antennas to detect wormhole attacks. Their approach uses a periodic HELLO message to determine the direction to each neighbor. When two nodes and wish to communicate, they find a correctly positioned "verifier" which ensures that the directions toward and are consistent. Their approach is promising; however, it relies on perfectly aligned, completely directional antennas, and cannot detect all wormhole instances, especially those using more than one wormhole.

M. A. Shurman, S. M. Yoo, and S. Park (2004) describe a protocol in which the source node verifies the authenticity of a node that initiates RREP by finding more than one route to the destination. When source node receives RREPs, if routes to destination shared hops, source node can recognize a safe route to destination. All solutions discussed above, involve additional overhead on either/both intermediate and destination nodes in one or the other way. Since the mobile nodes in MANETs suffer from limited battery life, processing power and storage, it is essential to devise a protocol that aims at reducing the overhead on intermediate and destination
nodes. In addition, the process of selecting secure root, should involve minimum possible rise in end-to-end delay.

Loanna Stamouli (2005) proposed RIDAN architecture which uses timed finite state machine to formally define attack against the AODV routing process. It uses a knowledge based methodology to detect the intrusion. RIDAN operates locally in every participating node and observe the network traffic. This model can able to detect resource consumption attack, sequence number attack and dropping routing packet attack.

Chiu and Lui (2006) proposed an AODV-based routing protocol, named DelPHI, to defend against wormhole attacks. DelPHI also applied a multi-path approach, and recorded the delay and hop counts in transmitting RREQ and RREP (actually named DREQ and DREP in DelPHI) through the paths. In this way, the average time taken by each hop can be calculated. In the case of a path subjected to wormhole attacks, the delay would be obviously longer than a normal path with the same hop count (i.e., the wormhole nodes may have a heavy load, and therefore, packet processing is slow). Hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided.

Lazos et al. (2005) proposed a graph theoretic model to characterize the wormhole attack and ascertain the necessary and sufficient conditions for any candidate solution to prevent wormholes. They used a Local Broadcast Key (LBK) based method to set up a secure ad-hoc network against wormhole attacks. In other words, there are two kinds of nodes in their network: guards and regular nodes. Guards access the location information through GPS or some other localization method like SeRLoc and continuously broadcast location data. Regular nodes must calculate their location relative to the guards’ beacons, thus they can distinguish abnormal transmission due to beacon retransmission by the wormhole attackers. All transmissions between
node pairs have to be encrypted by the local broadcast key of the sending end and decrypted at the receiving end. As a result, the time delay accumulates per node traveled. In addition, special localization equipment has to be applied to guard nodes for detecting positions.

A. Karygiannis, and A. Apostolopoulous (2006) proposed a method to detect the critical nodes for MANET. Critical node is a node whose failure or malicious behavior disconnects or significantly degrades the performance of the network. After identification of critical node, these nodes are continuously monitored. To detect the critical node they used a vertex cut and edge cut approach.

Xia Wang (2006) proposed end to end wormhole detection method in wireless ad hoc network. They used AODV protocol. In the route discovery process, the sender sets the Destination-only flag such that only the destination can be able to respond to the ROUTE REQUEST packet. Once the ROUTE REQUEST packet reaches to the destination, it responds by sending a ROUTE REPLY with its current position. The sender retrieves the receiver’s position from the ROUTE REPLY packet and estimates the lower bound of hops between the sender and the receiver. If the received route is the shorter than the estimated shortest path, the corresponding route will be discarded. Otherwise, the sender will select the shortest path corresponding to the estimation. After the detection of wormhole by sender, it temporarily enables the path with wormhole and send the TRACE packet to receiver through this path. This TRACE packet is forwarded by each intermediate node through the route with wormhole. When any node in the route receives the TRACE packet, it replies to sender by sending its current position and hop count to the destination node. Then the sender can calculate the increase of hop count at each node using the received position. If the increase of hop count at one node is not one comparing to its previous hop, then this node and its previous hop node are identified as the wormhole.
R. Ranjana and M. Rajaram (2007) proposed another model which does not perform any change in underlying protocol and used additional security component to detect fabrication attack, resource consumption attack and packet dropping attack.

Su and Boppana (2007) proposed a routing protocol to alleviate wormhole attacks. This protocol is a modification of the Ariadne (Hu et al., 2002) routing protocol, and can only defend against in-band (or packets encapsulated) channels of wormhole attacks. Their method calculates the average time in transmitting RREQ through normal nodes, so that a normal node can distinguish a particularly long duration in transmitting an RREQ when malicious nodes executing in-band wormhole attacks.

Naït-Abdesselam et al. (2007) used four message exchanges to defend against wormhole attacks in the Optimized Link State Protocol (OLSR) (Clausen and Jacquet, 2003) based routing protocol, as wormhole nodes should process a large amount of packets, causing longer delays of packets than in normal nodes. The authors mainly used Hello and ACK messages as the messages to confirm the delay.

Latha Tamilselvan, V Sankaranarayanan (2007) discuss an approach in which the requesting node waits for the responses including the next hop details, from other neighboring nodes for a predetermined time value. After the timeout value, it first checks in the CRRT (Collect Route Reply Table) table, whether there is any repeated next-hop-node or not. If any repeated next-hop-node is present in the reply paths, it assumes the paths are correct or the chance of malicious paths is limited. The solution adds a delay and the process of finding repeated next hop is an additional overhead.
S. Madhavi and Dr. Taj Hoon Kim (2008) developed another IDS for MANETs. In their work the author define the monitor node whose job is to detect misbehaving node. They also describe the algorithm for detecting the packet dropping and packet delaying attack.

Lee et al. (2008) proposed a scheme in which each node must broadcast messages that can be transmitted over 2 hops. Each node records the neighboring list of 1 hop and 2 hops, as well as the corresponding session keys. When a node received a routing message without a valid Message Authentication Code (MAC), there may be wormhole attacks. The purpose of maintaining a 2 hops neighboring list by each node is to allow the node to recognize if a wormhole attack is a hidden wormhole attack or an exposed wormhole attack, as wormhole nodes may reveal themselves or hide themselves in a routing path.

S. Sen (2009) proposed a “grammatical evolution approach for intrusion detection in mobile ad hoc networks”. They use artificial intelligence based learning technique to explore design space. The grammatical evolution technique inspired by natural evolution is explored to detect known attacks on MANETs such as DOS attacks and route disruption attacks. Intrusion detection programs are evolved for each attack and distributed to each node on the network.

Payal N. Raj, Prashant B. Swadas (2009) discuss a protocol viz. DPRAODV to counter the Blackhole attacks. DPRAODV checks to find whether the RREP_Seq_No is higher than the threshold value. In this protocol, the threshold value is dynamically updated at every time interval. If the value of RREP_Seq_No is found to be higher than the threshold value, the node is suspected to be malicious and is added to a list of blacklisted nodes. It also sends an ALARM packet to its neighbors with information about the blacklisted node. Thus, the neighbor nodes know that RREP packets from the malicious node are to be discarded. That is, if any node receives the RREP packet, it looks over the list to check the source of the received message. If
the reply is from the suspected node, the same is ignored. Thus, the protocol though successful, suffers from the overhead of updating threshold value at every time interval and generation of the ALARM packets. The routing overhead, as a result is higher.