Protection against wormhole attack using smart protocol in MANET

Kiruthika M.[1] and Premalatha J.[2]

1. Department of Computer Science and Engineering, Jansons Institute of Technology, Coimbatore 641 659, Tamilnadu, INDIA
2. Department of Information Technology, Kongu Engineering College, Perundurai, Erode 638 052, Tamilnadu, INDIA

Abstract

Wormhole attack forms one among the much crucial attack in MANET. In this attack, the malicious node attracts data traffic from the Source node, pretending to have a shortest route to the destination. The compromised nodes form a tunnel between them and when data packets start to flow between the tunnels, the packets are dropped or modified. Patient monitoring through mobile healthcare using wearable devices provides flexible care at any time and anywhere. The main challenges faced by healthcare providers is to secure the personal information of patients and maintain privacy concerns. In this paper, a novel technique using Smart Monitoring Agents for Reliable Transmission (SMART) protocol is proposed to detect the malicious nodes involved in wormhole attack. Trust value is assigned to all nodes within the range of the Smart Monitoring Agents. Route in-between the Source and the Destination is established on the basis of Trust value, Hop Count and Sequence Number. The Route Reply packet of AODV protocol is modified to include Trust value. The implementation is done using Network Simulator 2 (NS2) and the network performance in particular to wormhole attack is analysed under fluctuating number of malicious nodes. The results prove that the presented algorithm is good compared to other standard AODV protocols.

Keywords: Mobile ad hoc networks, AODV, Wormhole Detection, Packet Drop, Reliable.

Introduction

A Mobile Ad hoc Network (MANET) forms a progressing area of research, where there are no access points or routers. MANETs are infrastructure-less or self-forming networks, i.e., the nodes establish their own network topology [1]. These networks can be used in situations where infrastructure is unavailable, for instance, in military applications, in emergency situation, in urban sensing, in Internet of Things (IoT) applications, etc. In MANET, the nodes serve as both the hosts as well as the routers.

Unlike the Infrastructure based conventional network, routing process is difficult in MANET because routing needs cooperation among nodes. In order that a communication in-between the source as well as destination is established, a route is explored using routing protocols. The MANET routing protocols are categorized as Table-Driven (Proactive) routing protocols as well as On-Demand (Reactive) routing protocols [2] on the basis of routing table information update method. Proactive or Table-Driven routing protocols emphasis each node to periodically exchange routing information and accordingly make updates to the routing table. This routing table update is performed frequently so as to preserve network data accurately. Some popular examples of table-driven routing protocols are Destination Sequenced Distance-Vector (DSDV) routing protocol, Optimized Link State Routing (OLSR) protocol and Cluster-head Gateway Switch Routing (CGSR) protocol. These protocols are not suited for high dynamic networks due to the additional control overhead needed to keep the routing tables consistent [3]. In Reactive or On-Demand routing protocols, the routing information is exchanged in case a path is needed by a source node to transfer data to destination node. Since the routing information is gathered only when needed, the routing table is up-to-date in these protocols. Few examples of reactive routing protocols include Dynamic Source Routing protocol (DSR) and Adhoc On-demand Distance Vector routing protocol (AODV). Usage of these protocols will produce less overhead in maintaining the routes and the routes will be consistent. However, there may be initial delays incurred while obtaining the routes between source and destination.

Electronic healthcare (e-healthcare) and mobile healthcare (m-healthcare) has advanced in leaps and bounds in the recent years. Wireless devices and mobile networks allows medical professionals to operate in hands-free mode, while communicating with other colleagues in a hospital, wearable sensors enables e-healthcare making it possible for patients to be monitored from long distance. Both medical professionals and patients benefit from m-healthcare. The advances in wireless and mobile technologies makes m-healthcare and e-healthcare systems more realistic and feasible [4].

The portable and wearable sensors helps in monitoring the health status of a patient in realtime, then send the sensed data to the patient healthcare monitoring centres in an automated manner. Monitoring the patients serves to be the much significant foundation to m-healthcare. To make m-healthcare available to all lives, monitoring the patient takes the benefit of typical wireless as well as mobile networks, like the MANET as well as the Body Sensor Network (BSN), to work in fields which don’t have a pre-defined structure [5]. These networks could assist any number of patients it can and permit maximum patients’ mobility. Due to the absent of any constant infrastructure, communicating data in these networks entirely depend on the co-operation between the wireless devices. In case two of the medical sensors lie in each one's transmitting range, they could have direct communication; else, rest of the sensors or devices could co-operate to deliver the data transmitted. Hence co-operation between the nodes should be good and it needs much security.

Though, securing the data seems to be a needed component in the m-healthcare scheme, because many patients think about their privacy when they come across the idea of transmitting their private data over the wireless channels. Although real time monitor as well as data transmitting gives required data in a quick manner, it could also reveal medical information of a patient to malicious intruders and eavesdropper. In case a m-healthcare scheme doesn't have required security during data communication, unauthorized users could get hold of the patient's information, modify their medical history, inject incorrect data to the stream using a restricted node. Hence at the time of m-healthcare planning, considering security is inevitable because of the shared character of the wireless devices, patients' mobility as well as susceptibilities of prevalent and universal surroundings [6].

MANETs are more vulnerable to attacks caused by the internal nodes, because of the dependability on other nodes for routing. Though attacks are possible on different layers of MANET, the primary concern is towards the attacks on network layer. Network layer attack disrupts the routing process and is considered to be severe as the entire network can be paralyzed [7]. Wormhole attacks are severe in MANET as they are launched by compromised nodes and are difficult to detect.

In wormhole attack, the malicious node or nodes attract packets towards them by claiming to possess a shortest route towards the destination. The compromised nodes form a Tunnel (a Virtual Pipe) between them. After attracting the data packets, they can be eavesdropped or discarded. Wormhole attacks are mostly thrown against Reactive routing protocols like AODV or DSR.

The proposed technique to detect wormhole attack is by deploying Smart Monitoring Agents (SMAs) that assigns Trust values for nodes in its range. Also the SMART protocol detects the malicious wormhole nodes by selecting routes based on the Trust value, Destination Sequence number and Hop count. When the node is suspected, the Trust value is reviewed by the SMAs. If the node still proves to be malicious, keep the rust value as zero. This ultimately acts as an Intrusion Detection system, where the compromised node is blacklisted from further communication. In our paper, we have considered Ad hoc On-demand Distance Vector (AODV) routing protocol because AODV produces less end-to-end delay as well as less routing overhead in comparison with other reactive routing protocols [8].

The paper is formulated as below. In Section 2, the earlier works for protecting the MANET against wormhole attack in reactive routing protocols are discussed; Section 3 gives the methodology of the proposed work; Section 4 briefs out the experiment information as well as its examination with the help of NS2; and Section 5 concludes the work.

Related Works

Wormhole attack is one of the severe attacks of MANET and could have a serious impact on the Reactive routing protocols, like AODV or DSR. The malicious nodes form a tunnel between them and route the packets faster compared with other routes. Because of this feature, these nodes involve themselves in several routes. Once the traffic starts to flow through them, the malicious nodes either drops or modify the packets else send the packets to a third party malicious node [9]. The various wormhole detection methodologies / techniques proposed by many researchers can be classified roughly based on the following detection features:

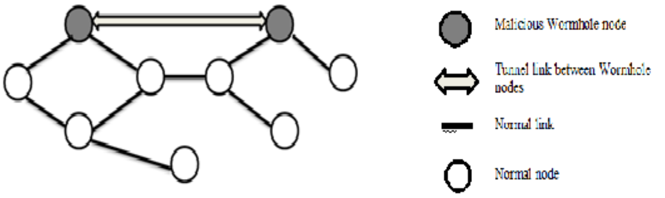

Fig. 1: Illustration of Wormhole Attack in MANET

Hu et al. [10] introduced a location based detecting and defending mechanism that uses TIK protocol with temporal or geographical leash. The technique needs the nodes to possess tighter sync clocks. A countermeasure against wormhole attacks having directional antennae was presented by *Hu and Evans* [11] that defends the attack packets based on the attack direction. The problem in this approach is that it may prevent some legitimate links from getting established.

Khalil et al. [12] presented a lightweight countermeasure known as LITEWORP that doesn't employ any special hardware and includes protocol to detect as well as isolate the malicious nodes. The node's traffic is monitored by the neighbouring nodes. *Chiu and Lui* [13] proposed a detection method named DelPHI (Delay Per Hop Indication) that detects the malicious node based on delays. The average time taken while transmitting RREQ and RREP packets by each hop is calculated by recording the delay and hop counts. The drawback of this method is the message overhead it incurs.

Su [14] proposed a technique called Wormhole Avoidance Routing Protocol – WARP that enables the neighbourhood nodes to gain knowledge about the wormhole nodes by observing abnormal path attractions. The wormhole nodes are quarantined slowly from the network by the neighbouring nodes. *Gupta et al.* [15] suggested a protocol called WHOP – Wormhole attack detection protocol using HOund Packet that counts the hop difference among the neighbours. The wormhole node is detected if the hop difference exceeds the acceptable level.

Chaurasia and Singh [16] modified the AODV protocol to detect the wormhole attack with the help of hops' amount as well as every node's delay across various routes in-between the source as well as destination. *Giannetsos and Dimitriou* [17] conferred a lightweight countermeasure called LDAC (Localized – Decentralized Algorithm for Countering wormholes) that detects wormhole using connectivity information. Patel *et al*. [18] devised a technique to detect as well as prevent wormhole using Hash based Compression Function (HCF) that computes the hash field in RREQ packet.

Proposed Methodology: The proposed model has the following assumptions. (a) All the mobile nodes have the same physical characteristics. (b) SMAs are set in promiscuous mode only when needed and are deployed at regular intervals. (c) Trust value of a mobile node is initially set to zero.

Protocol Description: In AODV protocol, the Source Node (SN) transmits the Route Request (RREQ) packet so as to determine a path to the required Destination Node (DN). Upon receiving the RREQ message, the intermediate nodes verify their Routing tables whether they possess path for the specified destination. In case, there is a route to the required destination, then the intermediate node will unicast a Route Reply (RREP) packet to SN. The route will be selected by the SN if the Destination Sequence Number (DSNUM) is fresh.The proposed method require the Route selection, not only based on the recent DSNUM, but also based on least Hop count (HC) and highest Trust value (TVal). The trust value is signed by the SMA using Digital Signatures. A fixed length message digest *d* is calculated using a pre-agreed hash function *H* for every TVal as follows:

$$H(TVal) = d \qquad (1)$$

SMA applies its own private key, PR_{SMA} on the message digest d as $E(PR_{SMA}, d)$. The TVal with the signature is sent along with the RREP packet. SN produces a hash code for the received TVal' using the same Hash function H. Let this value be noted as:

$$H(TVal') = d' \qquad (2)$$

The receiver can verify the signature by applying the Public key of SMA, PU_{SMA} on the message digest *d* as $D(PU_{SMA}, d)$. Now, the receiver knows both *d* and *d'*. If (1) and (2) are equal, then the receiver knows that the TVal is sent by the SMA indeed.

The malicious nodes which perform Wormhole attack will send the RREP packet correctly to the SN as other non-malicious nodes. These Wormhole nodes will specify that they have fresh DSNUM. To mitigate the Wormhole attack, the nodes have to send the RREPs along with TVal given by the SMA. Upon receiving the RREPs, the SN will invoke the SMART protocol. TD_{DS} is the threshold of the accepted difference between Destination Sequence Numbers. Method 1 shows the working of the SMART protocol.

Method 1: Action performed by SMART protocol

Step 1: Calculate the weight of the path, p, as $\boldsymbol{W(p) = \sum_{k=0}^{n} HC\,(k)}$

Step 2: Repeat Step 1 for all the possible RREPs received.

Step 3: Select two paths, P_1 and P_2 that have the least possible Weights.

Step 4: After selecting the least weighted paths, compare the values of D_{DS} and TVal.

Step 5: Calculate D_{DS} as difference between DSNUM (P_1) and DSNUM (P_2). TD_{DS} is set to a value between 0 and 2.

Step 6: If ((PD <= TPD) & (TVal (P_1) > TVal (P_2)), then select P_1 to be the correct path.

Step 7: Else if ((PD <= TPD) & (TVal (P_1) < TVal (P_2)), then select P_2 to be the correct path.

Step 8: Else an error report ER is sent to SMA tto recalculate the TVal of the Node.

SN finds the best path by running the above process. The Trust value to a node is incremented or decremented only by the SMAs based on the reports received from the nodes and Packet Delivery Ratio (PDR). PDR cache is maintained at each node as a counter value that is incremented when the packet is delivered correctly at the destination. PDRR is the report of Packet Delivery Ratio. Method 2 specifies the tasks performed by the SMAs to detect and isolate the Wormhole nodes.

Method 2: Action performed by SMA Nodes

Step 1: Collect PDR and ER from the nodes at specified time interval.

Step 2: If PDR and ER are below the already defined PDR and ER of that node, then the SMA decrements the TVal of the node by 1.

Step 3: Else the TVal is incremented by 1.

Step 4: When TVal reaches zero, then the node is blacklisted from the network.

Step 5: SMA broadcasts an ALARM packet to intimate the presence of attacker node in the network.

Simulation and Results

The simulation environment used is network simulator 2.34. The network area for simulation is set to 1000 × 1000 m with 50 AODV nodes, 50 SMART nodes and 10 SMA nodes that are distributed across the network area. The malicious

Wormhole nodes are set to 10 that perform Wormhole attack. The maximum transmission range is set to 250 m. Simulation time is set to 600s. The mobility model that is made use in Random Way Point (RWP) model in which each node pause for 15s. The data is sent between nodes using UDP-CBR, i.e. User Datagram Protocol – Constant Bit Rate. The packet size is 512 Bytes. Table 1 lists the major parameters of NS2 simulation experiment.

Table 1
Simulation Parameters

Simulation Property	Values
Coverage Area	1000 × 1000
Protocols for Routing	AODV, SMART
Number of AODV nodes	50
Number of SMART nodes	50
Number of SMA nodes	5
Number of Attack nodes	2,4,
Simulation time	600 s
Mobility Model with Pause time	Random Way Point (RWP), 15s
Traffic Capacity	UDP packets of 5KB, Data payload of 512 Bytes
Transmission Range	250 m
Traffic Type	UDP - CBR

The proposed work is compared with AODV protocol (normal AODV and AODV under attacks). The following performance metrics are considered to evaluate the working of presented protocol.

Wormhole Detection Rate (WDR): WDR is the ratio of the total number of data packets successfully detected to the total number of data packets attacked by Wormhole. WDR is calculated as:

$$WDR = \frac{ndp_{DE}}{ndp_{AT}}$$

Here, ndp_{DE} is the number of wormhole data packets detected and ndp_{AT} is the total number of data packets attacked by Wormhole. Fig. 2 clearly shows the WDR is higher in SMART protocol compared with WDR in AODV protocol. WDR graph increases with number of wormholes, since the probability of SMAs to identify attacker nodes increases. The proposed protocol shows better WDR compared to AODV protocol.

Packet Drop Rate (PDR): PDR is the ratio of the total number of data packets dropped by the malicious nodes to the total number of data packets sent. PDR is calculated as:

$$PDR = \frac{ndp_{DR}}{ndp_S}$$

Here, ndp_{DR} is the number of wormhole data packets dropped and ndp_S is the total number of data packets sent by the sender. Fig. 3 clearly shows the PDR in SMART protocol is lower compared with PDR in AODV protocol. PDR graph shows a decrease when the number of wormhole nodes are high. The SMART protocol shows lower PDR compared to AODV protocol.

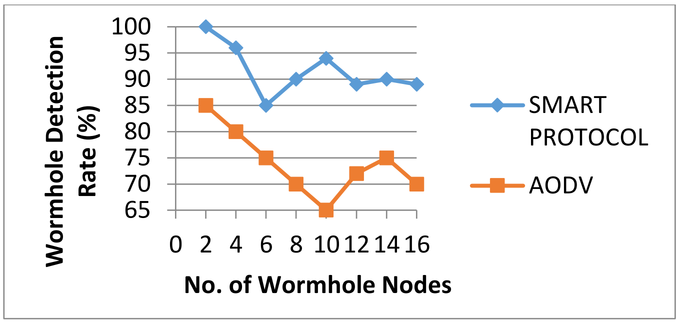

Fig. 2: Wormhole Nodes vs WDR

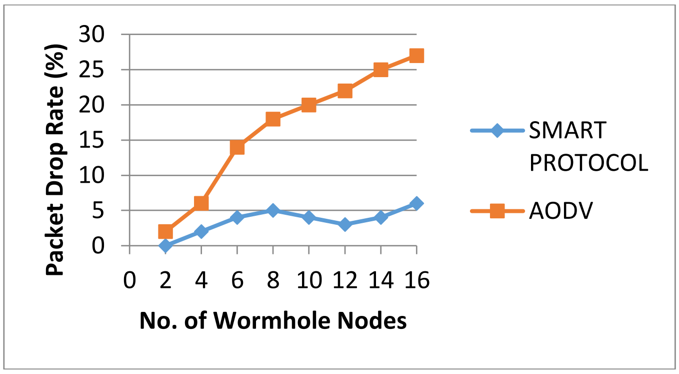

Fig. 3: Wormhole Nodes vs PDR

Wormhole Detection Accuracy (WDA): WDA is the ratio of the total number of nodes identified as malicious wormhole nodes to the total number of malicious wormhole nodes present. WDA is calculated as:

$$PDR = \frac{nwn_{DE}}{nwn}$$

Here, nwn_{DE} is the number of malicious wormhole nodes identified and nwn is the total number of malicious wormhole nodes present. Fig. 4 clearly shows that the percentage of accuracy in detecting wormhole nodes by SMART protocol is higher than the accuracy provided by the AODV protocol

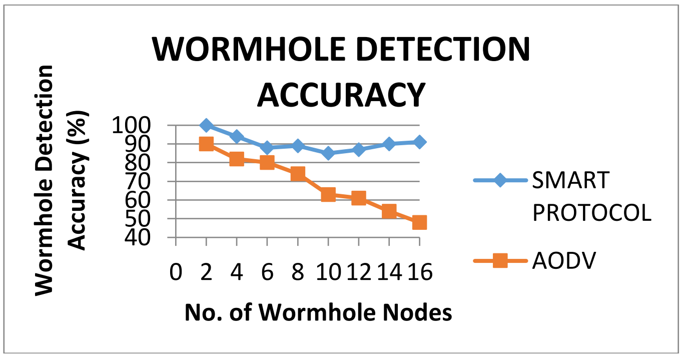

Fig. 4: Wormhole Nodes vs WDA

Conclusion

The proposed methodology is the design of SMART protocol that provides security in MANET against Wormhole attack. The protocol is compared with normal AODV in wormhole specific scenarios. Using this protocol, the MANET nodes can easily determine the malicious nodes that inject Wormhole attack into the network. With the help of trusted SMA nodes, simple intrusion detection is done by isolating the malicious node from the network. SMAs act in promiscuous mode, so as to save energy. The simulation result illustrates that SMART protocol is good compared to AODV protocol when considering Wormhole detection rate, Packet Drop rate and Wormhole detection accuracy.

References

1. S.Corson, J.Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETF Internet Draft, **(1999)**.

2. S. Murthy, C. S. Ram, B. S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall, **(2004)**.

3. A Boukerche, B Turgut, N Aydin, Mohammad Z. Ahmad, L Bölöni, D Turgut, Routing protocols in ad hoc networks: A survey, Computers Networks, **55**, 3032-3080, **(2011)**.

4. Ren, Y., Werner, R., Pazzi, N., & Boukerche, A., Monitoring patients via a secure and mobile healthcare system. IEEE Wireless Communications, **17(1)**, **(2010)**.

5. Wac, K., Bults, R., Van Beijnum, B., Widya, I., Jones, V., Konstantas, D., ... & Hermens, H., Mobile patient monitoring: the MobiHealth system. In Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE (pp. 1238-1241), **(2009)**.

6. Boukerche, A., & Ren, Y., A secure mobile healthcare system using trust-based multicast scheme. IEEE Journal on Selected Areas in Communications, **27(4)**, **(2009)**.

7. Praveen Joshi, Security issues in routing protocols in MANETs at network layer, Procedia Computers Science, **3**, 954 - 960, **(2010)**.

8. Abdul Hadi Abd Rahman and Zuriati Ahmad Zukarnain, Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks, European Journal of Scientific Research, 566-576, **(2009)**.

9. Muhammad Imrana, Farrukh Aslam Khanb, Tauseef Jamala, Muhammad Hanif Durada, Analysis of Detection Features for Wormhole Attacks in MANETs, Procedia Computer Science, **56**, 384-390, **(2015)**.

10. Hu, Yih-Chun, Adrian Perrig, and David B. Johnson, Wormhole attacks in wireless networks, IEEE journal on selected areas in communications, **24 (2)**, 370-380, **(2006)**.

11. Hu, Lingxuan, and David Evans, Using Directional Antennas to Prevent Wormhole Attacks, Network and Distributed System Security Symposium NDSS, **(2004)**.

12. Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff, LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks, IEEE International Conference on Dependable Systems and Networks - DSN 2005 Proceedings, 612-621, **(2005)**.

13. Chiu, Hon Sun, and King-Shan Lui, DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks, In Proc. International Symposium on Wireless Pervasive Computing, Phuket, Thailand, **(2006)**.

14. Su, Ming-Yang, WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks, Computers & Security, **29 (2)**, 208-224, **(2010)**.

15. Gupta, Saurabh, Subrat Kar, and S. Dharmaraja, WHOP: Wormhole attack detection protocol using hound packet, IEEE International Conference on Innovations in Information Technology (IIT), 226-231, **(2011)**.

16. Chaurasia, Umesh Kumar, and Varsha Singh, MAODV: Modified wormhole detection AODV protocol, IEEE Sixth International Conference on Contemporary Computing (IC3), 239-243, **(2013)**.

17. Thanassis Giannetsosa, Tassos Dimitriou, LDAC: A localized and decentralized algorithm for efficiently countering wormhole in mobile wireless networks, Journal of Computer and System Sciences, 618–643, **(2014)**.

18. Patel, Anal, Nimisha Patel, and Rajan Patel, Defending against Wormhole Attack in MANET, IEEE Fifth International Conference on Communication Systems and Network Technologies (CSNT), 674-678, **(2015)**.