A Review On Collaborative Decision Technique For Blackhole Attack Prevention In MANET

Shubha Dubey
Department of Computer Science& Engineering
RadhaRaman Institute of Tech & Science
chaturvedishubha07@gmail.com

Priyanka Saxena
Department of Computer Science & Engineering
RadhaRaman Institute of Tech & Science
saxenapriyanka12@gmail.com

Abstract- Mobile Ad Hoc Networks (MANETs) are collections of mobile nodes that can communicate with one another using multihop wireless links. MANETs are often deployed in the environments, where there is no fixed infrastructure and centralized management. The nodes of mobile ad hoc networks are susceptible to compromise. In such a scenario, designing an efficient, trustworthy and secure routing protocol has been a major challenge over the last many years. In this paper, we propose a Trust Based Secure On Demand Routing Protocol called "TSDRP". Ad hoc On-demand Distance Vector (AODV) routing protocol has been modified to implement TSDRP for making it secure to thwart attacks like Blackhole attack and DoS attack. To evaluate the performances, we have considered Packet Delivery Fraction (PDF), Average Throughput (AT) and Normalized Routing Load (NRL).

Keywords: MANETs, AODV, Routing Protocol, blackhole, Denial of Service, PDF, AT, NRL

1. Introduction

1.1 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. To support this connectivity nodes are use routing protocols such as AODV (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.

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. In recent years, application domains of mobile ad hoc networks have gained more and more importance in non military public organizations and in commercial and industrial areas. The typical application scenarios include rescue missions, law enforcement operations, cooperating industrial robots, traffic management, and educational operations in campus.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met [2]. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

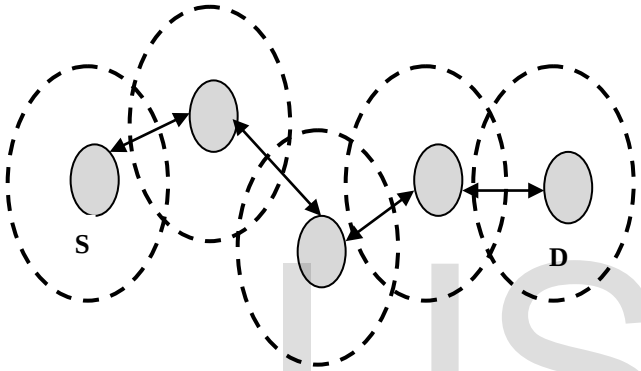

Fig.1.1 Ad hoc Network

1.1.1 NEED OF SECURITY IN AD HOC NETWORK

Though the ad hoc networks are widely used but still it has some vulnerability in it. Therefore, there is a need of security to defend such problems. An intruder utilizes this vulnerability to know about the network processes and then attack the network. Following are some present vulnerability in ad hoc networks.

- Mobility- Each node in ad hoc network is movable. It can join or leave a network at any instant of time without informing any node. This gives chance to intruder to easily enter in the network and even participating in its operations.
- Open Wireless Medium- All the communication between nodes is taking place through the medium of air instead of wires. An intruder can easily access this medium to gain information about the communication or can easily trap it.
- Resource Constraint- Every node in mobile ad hoc network has limited resources like battery, computational power, bandwidth etc. An intruder can unnecessarily waste these limited resources in order to make it unavailable to perform.
- Dynamic Network Topology- As the nodes are highly movable in nature, so the topology changes every time the communication takes place. The packets from source to destination may take different path for communication. An intruder can introduce itself in any path.
- Scalability- Ad hoc network may consist of number of nodes. This number is not fixed. In a network of its range, as many as number of nodes can take part. Intruder simply takes advantage of this parameter as there is no limitation on number of nodes.
- Reliability- All the wireless communication is limited to a range of 100 meter which puts a constraint on nodes to be in range for establishing communication. Due to this limited range, some data errors are also generated. For attacking a particular node, an intruder needs to be in its range.

1.2 BLACKHOLE ATTACK

In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. On receiving the request the malicious node sends a fake reply with extremely short route. Once the node has been able to place itself between the communicating nodes, it is able to do anything with the packets passing between them.

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting

node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

1.3 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.

1.3.1 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:

1.3.2 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.
Network either as internal, external or/ as well as active or passive attack against the network.

A. Internal Attacks Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them.

B. External Attacks These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication

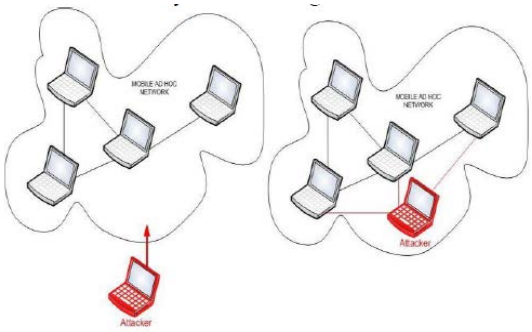

Fig1.2: External & Internal Attack in MANETs

2. LITERATURE SURVEY

We are doing a work on attacks mentioned in Akshai Aggarwal, Savita Gandhi et. al. [1] "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs" in that work they proposed a Trust Based Secure On Demand Routing Protocol called "TSDRP". Ad hoc On-demand Distance Vector (AODV) routing protocol has been modified to implement TSDRP for making it secure to thwart attacks like Blackhole attack and DoS attack. To evaluate the performances
"Harjeet Kaur1, Manju Bala , Varsha Sahni"[3] These protocols can be classified into three main categories reactive (on-demand), proactive (table-driven) and hybrid routing protocols namely AODV, OLSR and ZRP. This research effort focused first the comparative investigations of routing protocols under the various types of attack then to create scenario and simulate and investigate the performance metrics viz. Packet delivery ratio, average jitter, average throughput and end to end delay of reactive, proactive and hybrid routing protocols such as AODV and AODV with black hole attack, OLSR and OLSR with black hole attack and ZRP and ZRP with black hole attack for the different scenario under the different conditions.
Choi et al. in [4] 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 [5], 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. [6] may be considered.

In [7], 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 [8], 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 [9]. The rule-match approaches maintaining per flow state and matching packets to a pre-defined set of rules [10] has shown a certain good capability. However, rule-match approaches unlikely detect unknown DDoS attacks.

Lakhina et a1. [11] 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. [12] 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. [13] 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. [14] [15] 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) [16] 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 [17]. 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 [18] 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.[19] 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.

3.Performance Evaluation

There are following different performance metrics have been considered to make the comparative study of these routing protocols through simulation.

1) Routing overhead: This metric describes how many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets.

2) Average Delay: This metric represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination. It is measured in seconds.

3) Throughput: This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps

4) Packet Delivery Ratio: The ratio between the amount of incoming data packets and actually received data packets.

5) Blackhole Node Detection: Check the behaviour of generated profile and if detect the profile is not match with normal behaviour than identified the node number and time of capture the data file that gives the blackhole attacker node

6) Total Data Capturing Analysis by Black Hole Node: in this parameter we calculate total number of data captured by the blackhole node that help to calculation of percentage of attack in the network.

7) Security Percentage Measurement: after getting the blackhole node information we collaborative set prevention node that protect the data capturing and blocking the data from attacker, that helps to calculate network parameter and provide percentage of security, presence of blackhole node.

4 CONCLUSION

We have discussed some important an exhaustive simulation for MANET will done by using AODV routing protocols and the effect of the presence of black hole will also simulated. Significant QoS parameters such as throughput, delay, node density and packet delivery ratio. The study focuses on how performance of network will affected under black hole attack 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 the black hole attack.

REFERENCE

[1] Akshai Aggarwal et. al. “Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs” 2014 Fourth International Conference on Advanced Computing & Communication Technologies, 978-1-4799-4910-6/14 2014 IEEE DOI 10.1109/ACCT.2014.95

[2] Irshad Ullah* and Shahzad Anwar “Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols” IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, May 2013.

[3] Harjeet Kaur , Manju Bala , Varsha Sahni “Study of Black hole Attack Using Different Routing Protocols in MANET” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] H. Ringerg, A. Soule, J. Rexford and C. Diot, "Sensitivity of pc a for traffic anomaly detection", SIGMETRICS, 2007.

[13] 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.

[14] 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.

[15] 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.

[16] D. A. Maltz and D. B. Johnson and Y. Hu. The dynamic source routing protocol (DSR) for mobile ad hoc.

[17] L. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks,” in Proceedings of the Network and Distributed System Security Symposium.

[18] 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).

[19] Y. C. Hu, A. Perrig, and D. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in INFOCOM, 2003.