www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13047-13054

Design And Development Of Algorithm To Avoid Wormhole Attacks In Wireless Networks For Proactive Algorithms

Deepika D Pai

Abstract

Mobile Adhoc Networks (MANETS) allows portable devices to establish a communication independent of a central infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes.MANETS are vulnerable to many security attacks because of shared channel, insecure operating environment, lack of central authority, limited resource availability, dynamically changing network topology and resource constraints. Among the different attacks at the different network layers the wormhole attack is the most malicious. In this work, the wormhole attack is implemented in three different modes i.e. all pass, all drop and threshold mode with varying network sizes. Due to a highly dynamic environment routing in MANETS is a critical task. To make the network reliable we need efficient routing protocols. The routing protocols are of three kinds i.e. Proactive, reactive and hybrid. Four proactive protocols(DSDV, OLSR ,WRP,GSR,TBRPF) are analyzed in the presence of the worm hole attack considering four parameters which are throughput, average end-to-end delay, average jitter and packet delivery ratio in mobility and non-mobility domain.

Introduction

A Wireless ad-hoc network is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes.

In Wireless Sensor Networks, the nodes use the open air medium to communicate with each other, in doing so they face sensitive security problems as compared to the wired networks. One such dangerous problem is wormhole attack. In this attack, two distant malicious nodes can plan together using either wired connection or directional antenna, to give a feeling that they are only one hop away. Wormhole attack can be executed in hidden or in sharing mode. Wormholes can either be used to examine the traffic throughout the network or to crash packets selectively or totally to affect the flow of information. The security mechanisms that are used for wired systems such as authentication and encryption are useless under hidden mode of wormhole attack because the nodes do not modify their headers but only forward these packets. But the attack in participating mode is more

The lack of a backbone infrastructure coupled with the fact that mobile Ad Hoc networks change their topology frequently and without prior notice makes packet routing in ad-hoc networks a challenging task. The suggested approaches for routing can be divided into topology-based and position-based routing. Topology-based routing protocols use the information about the links that exist in the network to perform packet forwarding. They can be further divided into proactive, reactive, and hybrid approaches.

Proactive algorithms employ classical routing strategies such as distance-vector routing (e.g., DSDV) or link-state routing (e.g., OLSR and TBRPF). They maintain routing information about the available paths in the network even if these paths are not currently used. The main drawback of these approaches is that the maintenance of unused paths may occupy a significant part of the available bandwidth if the topology of the network changes frequently. In response to this observation, reactive routing protocols were developed (e.g., DSR, TORA, and AODV).

Reactive routing protocols maintain only the routes that are currently in use, thereby reducing the burden on the network when only a small subset of all available routes is in use at any time. However, they still have some inherent limitations. First, since routes are only maintained while in use, it is typically required to perform a route discovery before packets can be exchanged between communication peers. This leads to a delay for the first packet to be transmitted. Second, even though route maintenance for reactive algorithms is restricted to the routes currently in use, it may still generate a significant amount of network traffic when the topology of the network changes frequently. Finally, packets en route to the destination are likely to be lost if the route to the destination changes.

Hybrid Ad Hoc routing protocols such as ZRP combine local proactive routing and global reactive routing in order to achieve a higher level of efficiency and scalability. However, even a combination of both strategies still needs to maintain at least those network paths that are currently in use, limiting the amount of topological changes that can be tolerated within a given amount of time.

Position-based routing algorithms eliminate some of the limitations of topology-based routing by using additional information. They require that information about the physical position of the participating nodes be available. Commonly, each node determines its own position through the use of GPS or some other type of positioning service. A location service is used by the sender of a packet to determine the position of the destination and to include it in the packet's destination address. The routing decision at each node is then based on the destination's position contained in the packet and the position of the forwarding node's neighbors. Position-based routing thus does not require the establishment or maintenance of routes. The nodes have neither to store routing tables nor to transmit messages to keep routing tables up to date. As a further advantage, position-based routing supports the delivery of packets to all nodes in a given geographic region in a natural way. This type of service is called geocasting. Regardless of the approach to routing, a routing protocol should be able to automatically recover from any problem in a finite amount of time without human intervention.

Conventional routing protocols are designed for nonmoving infrastructures and assume that routes are bidirectional, which is not always the case for ad-hoc networks. Identification of mobile terminals and correct routing of packets to and from each terminal while moving are certainly challenging.

Literature Survey

For the proposed work idea thorough literature survey is done. Quality time is spent on reading reference books and papers to decide the title as well as objective of the proposed work.

Wormhole attack is the one of the major network layer attack of MANETs. In order to deduce the best suited protocol for wormhole attacked network, researchers employed detailed analysis of different protocol categories with varying the various simulation parameters. This section presents the existing background and related work of analysis of various protocols under wormhole attack in MANETs.

There have been various studies on analysis of proactive and hybrid protocols under mobility and non-mobility domain in the various journals.

Shaheen Khan *et.al* [1] analyzed a performance comparison of AODV (Ad-Hoc on Demand Distance Vector) Routing Protocol and Proactive includes DSDV (Destination Sequences Distance vector) Routing Protocol on the basis of Average End to End Delay, Network Load, Throughput and Packet Delivery Ratio (PDR) metrics by using Riverbed (OPNET) Simulator and revealed that DSDV outperforms AODV Routing Protocol in the Throughput and Packet Delivery Ratio (PDR) performance metrics. It also outperforms another protocol when deployed in high load networks. DSDV has shown the worst performance in packet End-to-End Delay and Network Load. It is therefore well suited for high capacity networks. The choice of a particular Routing Protocol will depend on the intended use of the network.

Kiranveer Kaur *et.al* [4] investigated the performance analysis of routing protocols AODV, DSR and OLSR protocols in MANET. The investigation considers the impact of scalability, mobility and network. HTTP, FTP and Email and Video Conferencing heavy traffic load on different types of routing protocols is taken. The simulation is done using OPNET .It is concluded the throughput of OLSR is higher than that of the reactive routing protocols AODV, DSR; it is because the OLSR protocol is independent of the traffic and network density compared to AODV, DSR protocols. The simulation results according to web application conclude that throughput is highest in HTTP and lowest in video conference and Email.

Sadeghi*et.al* [8] studied the effects of Wormhole attack on MANET in OPNET simulator using both Proactive routing protocol (OLSR) and Reactive routing protocol (AODV). Analyzing the throughput, end-to-end delay, network load and traffic received with wormhole and without wormhole on AODV protocol and OLSR protocol in MANET reveal AODV protocol is more vulnerability to wormhole attack as compared to OLSR protocol and concluded that the use proactive routing protocol is more trusted as compared to the reactive one.

Studies under [5], [2], [3], present the analysis carried out with variation of mobility speed and network size.

Sundararajan*et.al* [5] tested performance of seven different routing protocols (AODV, DSR, ANODR, DYMO, OLSR, OSPF, LANMAR) in variable network sizes with and without wormhole attack. The performances of all protocols were decreased because huge amount of system resources and processing power needed when network size increases. In homogeneous networks among on demand routing protocols DYMO protocol performs 21.5% well. Among other protocols LANMAR protocol performs 12.9% well. In heterogeneous networks among on demand routing protocols, DYMO protocol performs about 18.4% well. Among other protocols LANMAR protocol is performing 9.4% well. When there is an attack overall performance reduced about 20.1%.The packet delivery ratio in homogeneous network was 33% greater than homogeneous networks because in homogeneous network there is no different devices, no different frequencies and no different interfaces needed hence packet delivery ratio is more. The average end to end delay in heterogeneous network is greater than homogeneous network by 8%.

M.Senthil Kumar et.al [2] evaluated the performance of three routing protocols FSR, AODV and ZRP. He concluded AODV is a pure reactive protocol while FSR is a proactive and ZRP behaves as a proactive for higher routing zone. From simulation it was observed that AODV has performed well compared to all other protocols in terms of Average end – to – end delay, Packet Delivery Ratio and System Throughput. FSR and ZRP fails to respond fast enough to changing topology as compared to AODV. The performance of ZRP can be increased by incorporating other protocols in it. FSR is more desirable for large mobile networks where mobility is high and the bandwidth is low.

Shefali Garg et.al [3] compared two on-demand routing protocols i.e. AODV and DSR. On the basis of performance of protocols with varying number of nodes, the throughput of DSR is high as compared to AODV protocol. AODV protocol has minimum throughput and maximum end to end delay. As per performance analysis of both routing protocols on the basis of various parameters (Throughput and End to End Delay), it is concluded that DSR protocol is best performer as compared to AODV. On the basis of performance of protocols with varying pause time, again the throughput of DSR is high as compared to AODV protocol. From different analysis of graphs and simulations it is concluded that DSR performs well than AODV under different situations with variation in pause time.

Following studies under [6], [7] and [10] present the analysis carried out with variation of pause time.

Gurjinder*et.al* [6] analyzed the AODV and DSR protocol in three different modes of wormhole attack (All Pass, All Drop, Threshold) using Qualnet simulator and revealed that AODV protocol throughput is greater than DSR protocol in all pass and all drop mode while DSR protocol throughput is higher than AODV protocol in threshold mode.

Amrit*et.al* [7] investigated the AODV, DYMO and FISHEYE protocol by varying the pause time and by varying the node speed individually under the scenario of 50 nodes in Qualnet simulator and concluded that in former case, AODV protocol shows good response other than two protocols and in later case, DYMO protocol shows notable response as compared to other two protocols.

Bisen*et.al* [10] evaluates three on-demand routing protocols named as DYMO, AODV and DSR protocols with variation in pause time for mobile ad-hoc networks using Qualnet simulator and concluded that DSR protocol performs well than AODV protocol and DYMO protocol under different situations with variation in pause time. Because of enhanced version of AODV protocol, DYMO protocol shows better performance than AODV protocol.

Following studies under [9] and [11] present the analysis carried out with variation of traffic load and packet size.

Nand*et.al* [9] analyzed the AODV, DSR and DYMO protocols with variation of traffic load and concluded that AODV protocol outperforms both of the DSR and DYMO routing protocols in terms of the packet delivery ratio as it uses fresh routes and DSR protocol performs poorer because of aggressive use of cache. The DYMO protocol shows best throughput as it avoids good routes and outperforms than both DSR and AODV protocols and performs better with heavy load. The DSR protocol reflects poor performance due to absence of proper mechanism to expire the stale routes which further results in high jitter and average end-to-end delay in comparison to AODV and DYMO protocols.

Odeh*et.al* [11] evaluates MANET's performance for two proactive protocols named as AODV and DSR protocols with respect to packet size using network simulator NS2 and reveals that DSR protocol has shown better performance in terms of efficiency for a packet size less than 700 bytes. Both protocols show comparable results for other performance metrics: Propagation time and Drop rate.

Motivation and Problem Identification

Current threats against MANETs are becoming more and more sophisticated so that prevention solutions based on single attacks may no longer be sufficient. In MANETs, the identification of malicious activity is difficult when one node misbehaves during route formation. Further, if multiple malicious nodes collude together to perform malicious acts, their activity becomes even harder to detect. If multiple nodes act maliciously, simultaneously or alternatively to launch wormhole attacks, the schemes used to deal with them become less efficient and less effective at warding off these attacks.. Mobile Ad Hoc networks (MANETs) are vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed operation and constrained capability. Security and robustness will impact the design of the standard for Ad Hoc networks is the main motivation for this thesis.

The method for analyzing the routing protocols traffic is to begin with a carefully designed base configuration and network scenario for the experiment, and to vary the node density and mobility at a time to stress the network in different directions. Careful selection of these control parameters enables us to assess and isolate the effect of network size, with fixed application traffic CBR. In addition, design of the base condition, network topology, and routing are to be taken into account the real networks for which the results should be applicable.

Till now the analysis has been carried out with reactive protocols only, wormhole attack can also be analyzed with proactive protocols and hybrid protocols. Analysis can also be carried out with different mobility models. Proactive protocols, reactive protocols and hybrid protocols can also be analyzed under wormhole attack with varying the mobility speed and varying the pause time.

Objectives

The main objective of this work is to analyze the performance of reactive protocols under wormhole attack in both mobility and non-mobility domain. Following are the objectives:

□ To implement the wormhole attack with different modes.

 To simulate the various proactive routing protocols under wormhole attack in mobility and non-mobility domain.

 To analyze the performance of protocols under wormhole attack in mobility and non-mobility domain

Methodology

Wormhole nodes in varying network size are inserted. Values of all four parameters (Throughput, Average delay, Average jitter and Packet delivery ratio) are noted with varying the wormhole modes and protocols under both mobility and non-mobility domain. With increasing the network size, parameters values are noted with varying the wormhole modes and protocols under both mobility and non-mobility domain and graphs are analyzed.

A. Wormhole Modes in Qualnet

Following are the three different modes for the wormhole:

(1) THRESHOLD: In this mode, nodes connected to wormhole subnet drop any packet with size greater than or equal to the threshold value.

(2) ALL PASS: In this mode, nodes connected to wormhole subnet pass all packets irrespective of their size. This mode will pass all packets which are routed through node by not considering packet size. It is one of the best mode as all packets are passed without any active/passive attacks on packets.

(3) ALL DROP: In this mode, nodes connected to wormhole subnet drop all packets irrespective of their size. This mode will always drop packets which are routed through node.

.

B. Wormhole Sample Scenario

Figure below represents the scenario in which 20 nodes are connected to different subnets. Subnet marked with arrow behaves as wormhole subnet. Any node connected to this subnet will behave as wormhole nodes as according to the wormhole mode set by user.

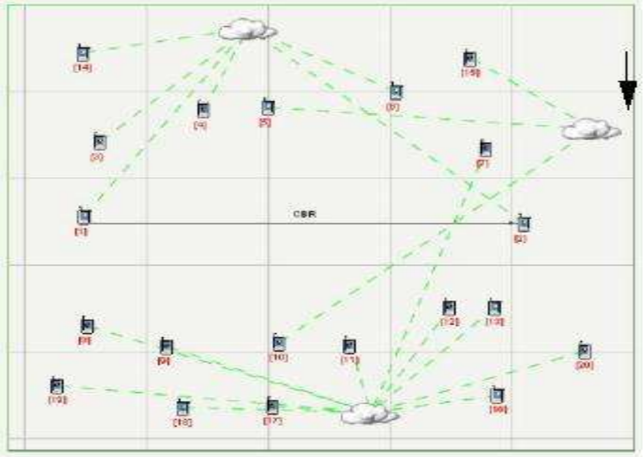

Figure: Wormhole Sample Scenario

C. Performance Metrics for Evaluation

In this work, four network parameters will be measured in simulations. The outcomes of these parameters reveals the best routing protocol suited for wormhole attacked network. The parameters are defined as follows:

(1) Throughput: It is the measure of the number of packets successfully transmitted to the final destination per unit time. It is measured in bits per second i.e. bits/sec or bps. Mathematically, it is calculated as

Throughput (bps) = Number of (Bits or Packets) Transferred/ time

(2) Average End-to-end delay: It is defined as

the average time taken by packets to reach the destination end from the source end.

(3) Average Jitter: It signifies that the Packets reach the destination with different delays. It is most significant factor of quality of Service for assessing network performance

(4) Packet delivery ratio: It is the ratio of number of packets received by the destination through the number of packets originated.

Mathematically, PDR is calculated as

PDR= Number of packet Received/ Number of packet originated.

References

[1] Shaheen Khan, Dr. Javed Khan Bhutto, Gautam Pandit, "Reactive and Proactive Routing Protocol Performance Evaluation for Quantitative Analysis in MANET", IJSRE, Volume2, Issue12, pp2540-2551, December 2014.

[2] M.Senthil Kumar, Dr.R.Asokan, "Impact of Node Density and Pause Time on the Performance of Ad Hoc Routing Protocols" GESJ: Computer Science and Telecommunications, 2010.

[3] Shefali Garg,Ranjith Singh Chauhan, "Comparative study of ADHOC routing protocols AODV&DSR in Mobile ADHOC Networks" IJCSCE Special issue on "Emerging Trends in Engineering" ICETIE 2012 .

[4] Kiranveer Kaur, Surinderjit Kaur, Vikramjit Singh "Throughput Analysis of Proactive and Reactive MANET Routing Protocols " International journal of Emerging Research in Management and Technology,ISSN:2278-9359(Vol-3,Issue-3),March 2014.

[5] T.V.P. Sundararajan, Karthik, A. Shanmugam, "Security and Scalability of MANET Routing Protocols in Homogeneous & Heterogeneous Networks", Proceedings of the International Conference on Man-Machine Systems (ICoMMS), 11 – 13 October 2009, BatuFerringhi, Penang, MALAYSIA

[6] GurjinderKaur, V.K.Jain, YogeshChaba, "Wormhole Attacks: Performance Evaluation of On Demand Routing Protocols in Mobile Adhoc Networks", World Congress on Information and Communication Technologies, IEEE, 2011.

[7] AmritSuman, PraneetSaurabh, BhupendraVerma, "A Behavioral Study of Wormhole Attack in Routing for MANET", International Journal of Computer Applications (0975 – 8887), Volume 26– No.10, July 2011.

[8] Mohammad Sadeghi, Prof. Dr.SaadiahYahya, "Analysis of wormhole Attack on MANETs Using Different MANET Routing Protocols", ICUFN, IEEE, 2012, pp. 301-305.

[9] Parma Nand, Dr. S.C. Sharma, "Performance study of Broadcast based Mobile Adhoc Routing Protocols AODV, DSR and DYMO", International Journal of Security and Its Applications, Vol. 5 No. 1, January, 2011.

[10] DhananjayBisen, PreetamSuman, Prof. Sanjeev Sharma, Rajesh Shukla, "Effect of Pause Time on DSR, AODV and DYMO Routing Protocols in MANET", IJITKM, 2009.

[11] AmmarOdeh, EmanAbdelFattah and MuneerAlshowkan, “Performance Evaluation of AODV and DSR routing Protocols in MANET Networks”, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012.