International Journal for Rapid Research in Engineering Technology & Applied Science
ISSN (Online): 2455-4723
Vol 3 Issue 2 February 2017

A Review Based on Black-hole and Wormhole Attack on Trust Based Approach in MANET

Monika Labana*,Mr.Mohit Jain**
Research Scholar, BM College of Science & Technology, Indore, M.P, India*
Department of Computer Science & Engineering

monica.it1990@gmail.com*,bmctmohitcs@gmail.com**

Abstract: Security is very essential in both wired and wireless network communication. Network security is an important criterion for wired and wireless communication. The advancement in wireless technologies and the high availability of wireless equipment in everyday devices is a factor in the success of infrastructure-less networks. MANETs are becoming more and more common due to their ease of deployment. The high availability of such networks and the lack in security measures of their routing protocols are alluring a number of attackers to interrupt. An ad hoc network is a collection of number of wireless computers having dynamically changing topology due to which the security issues are more in case of wireless networks. In recent year with the widespread use of mobile device, Mobile Ad hoc networks (MANETs) technology has been attracted attention day by day. In this paper, our aims to propose a trust based model for defending network from the severe types of network attack i.e. black-hole and wormhole attack. So this paper present the survey analysis of the existing approaches based of attack prevention.

Keywords:MANET, AODV, Wormhole, Black-hole, Security, Wireless Communication, Trust

IIntroduction

Ad-hoc networks are a key in the evolution of wireless networks [1]. Ad-hoc networks are typically composed of equal nodes, which communicate over wireless links without any central control. Although military tactical communication is still considered as the primary application for ad-hoc networks, commercial interest in this type of networks continues to grow. Applications such as rescue missions in times of natural disasters, law enforcement operation, commercial and educational use, and sensor networks are justfew possible commercial examples. Ad-hoc wireless networks inherit the traditional problems of wireless and mobile communications, such as bandwidth optimization, power control and transmission quality enhancement. In addition, the multi-hop nature and the lack of fixed infrastructure generate new research problems such as configuration advertising, discovery and maintenance, as well as ad-hoc addressing and self-routing.

A mobile ad hoc network, such as the one shown in Figure 1, is a collection of digital data terminals equipped with wireless transceivers that can communicate with one another without using any fixed networking infrastructure. Communication is maintained by the transmission of data packets over a common wireless channel. The absence of any fixed infrastructure, such as an array of base stations, makes ad hoc networks radically different from other wireless LANs. Whereas communication from a mobile terminal in an “infrastructured” network, such as a cellular network, is always maintained with a fixed base station, a mobile terminal (node) in an ad hoc network can communicate directly with another node that is located within its radio transmission range [2].

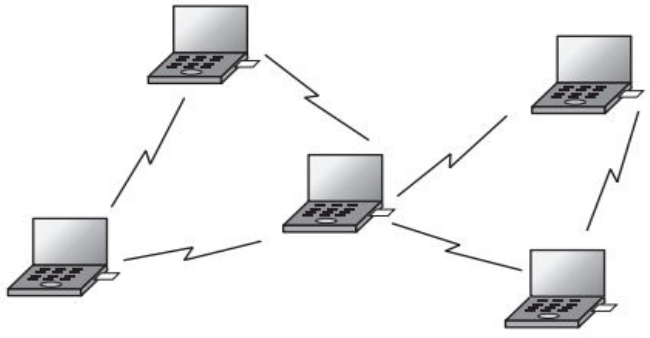

Figure 1: Mobile ad hoc network [2]

A. Trust Mechanism

Trust mechanism is introduced in the protocols to provide security in MANET. Trust is a value that is calculated on the basis of nodes action when needed. Trust is introduced to prevent from various attacks like wormhole, black-hole, Dos, selfish attack etc. Trust can be implemented in various ways such as by reputation, subjective logic, from opinion of nodes etc. as there are no particular definitions of trust. Following properties of the trust mechanism are [3]:

Context Dependence: In some specific context trust relationships are applicable.

Function of uncertainty: Trust depends on the uncertainty of nodes action. It gives the probability of action performed by a node.

Quantitative value: Trust can be assigned any type of numeric values discrete or continuous.

Asymmetric Relationship: Trust relationship is asymmetric in nature. If node A trusts B and node B trust C that does not mean that A trusts C. There are some different representations of trust. Basically, they can be divided into two categories-continuous and discrete numbers. Trust value can be of different ranges. For example, trust value can be continuous number 0,1,2,3 where different trust levels are assigned to that continuous values i.e. 0 means no trust, 1 means suspected and so on

The remainder of paper is organized as follows. Section 2 describes related work and Section 3 is short study about Wormhole and Black-hole Attack. In Section 4, proposed scheme is discussed for making MANET free from the malicious attack. Finally conclusion is discussed in section 5.

II Literature Survey

Numerous Researchers have worked on multiple detection and prevention of black-hole and wormhole attacks in wireless ad-hoc network, based on the detection mechanism, the existing techniques of detecting and preventing wormhole attacks can be illustrate in this section.

In this paper, Poonam Gera et al. [4] propose a novel method to enhance security in both phases using trust-based multi-path routing. The trust based multi-path routing ensures secure discovery of multiple path between source and destination. Self-encrypted parts of a message are transmitted through these paths. Therefore it is difficult for malicious nodes to gain access to the minimum information required to break through the encryption strategy. Results show in this method is much more secure than other existing trust based multipath routing protocols.

Wormhole attack is one of the most destructive severe attack in which malicious node captures the traffic at particular location and tunnels it to another part of tunnel that is far away. In network security is generally equated by strong and feasible authentication and adopting methods of encryption and decryption. However this attack is hardly defeated as they do not use any additional effort to deploy nor create any extra packets. They simply capture packets then either drop them or replay in existing network, which make them to pass from any type of cryptographic checks and authentication Work done in this field have generally focused on use of additional hardware like directional antenna. In this paper, Kamini Singh et al. [5] present a cluster based counter-measure for the wormhole attack that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET. Simulation results shown on NS2 display the effectiveness of the proposed method for detecting and preventing wormhole attack.

Self-configuring nature of MANET exposes itself to variety of active and passive attacks. Black hole attack is an active attack which creates disruption in communication path. There are two types of black hole attack i.e. single black hole attack and collaborative black hole attack. Authors have considered single black hole attack. In this paper, single malicious node doesn't allow the transmission of legitimate packets to the receiver and drop that packet. In this work in trust Priyanka Donga et al. [6] present a detailed survey on various trust computing approaches and this approaches are used find the black hole attack in MANET.

Mobile Ad hoc Networks (MANETs) are autonomous mobile node systems connected by wireless links. A node operates as an end system and as a router, to forward packets. MANET routing is challenging and has received tremendous attention from researchers. Dynamic Source Routing (DSR) protocol was accepted as a dominant routing protocol for MANETs. Performance analysis and results are show that DSR as an outstanding routing protocol consistently outperforming other routing protocols. In this paper, Mahamuni, K et al [7] proposes a new, secure DSR protocol for MANETs based on trust and reputation to mitigate black hole attacks.

This work analyses the black hole and cooperative black hole attack which is one of the new and possible attack in ad-hoc networks. A black hole is a type of attack that can be easily employed against routing in mobile ad-hoc networks. In this attack a malicious node advertises itself

as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. This solution discovers the secure route between source and destination by identifying and isolating black hole nodes. In this paper, via simulation, N. Bhalaji et al. [8] evaluate the proposed solution and compare it with standard DSR protocol in terms of throughput, Packet delivery ratio and latency. They have conducted extensive experiments using the network simulator-2 to validate our research.

Ad hoc networks typically work in an open un-trusted environment with little physical security, they are subject to a number of unique security attacks like wormhole attack. The wormhole attack is considered to be a serious security attack in multi-hop ad hoc networks. In wormhole attack, attacker makes tunnel from one end of the network to the other, nodes stay in different location on two ends of tunnel believe that they are true neighbours and makes conversation through the wormhole link. Unlike many other attacks on ad-hoc routing, a wormhole attack cannot be prevented with cryptographic solutions because intruders neither generate new, nor modify existing, packets, but rather forward existing ones. In this paper a simple technique to effectively detect wormhole attacks without the need for special hardware and/or strict location or synchronization requirements is proposed. The proposed technique makes use of variance in routing information between neighbours to detect wormholes. The base of dissertation is to find alternative path from source to second hop and calculate the number of hops to detect the wormhole.

Ad-hoc Networks (MANET) are self-organizing, decentralized networks and possess dynamic topology, which make them attractive for routing attacks. Wormhole attack is a network layer attack observed in MANET, which completely disrupts the communication channel. In this paper, Vandana, C et al. [10] focuses on study of wormhole attack, its behavior and the performance impact of wormhole attack on Ad-hoc On Demand Distance Vector (AODV) routing protocol. The NS2 network simulator is used to evaluate the wormhole attack impact on AODV.

III Attack Study

A. Wormhole Attack

Scarcity of various resources makes wireless sensor network vulnerable to several kinds of security attacks. Attacker possessing sufficiently large amount of memory space, power supply, processing abilities and capacity for high power radio transmission, results in generation of several malicious attacks in the network. Wormhole attack is a type of Denial of Service attack that misleads routing operations even without the knowledge of the encryptions methods unlike other kinds of attacks. This characteristic makes it very important to identify and to defend against it [11].

The two malicious end points of tunnel may use it to pass routing traffic to attract routes through them. Wormhole nodes can disrupt the data packets which results in unnecessary routing activities by turning off the wormhole link periodically. The attacker can simply record the traffic for later analysis. An attacker can also break any protocol that directly or indirectly relies on geographic proximity [12]. In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network where these packets are resent into the network.

This tunnelling between two colluding attackers is referred to as a wormhole. Wormhole establishment is possible through wired link between two colluding attackers. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel [12].

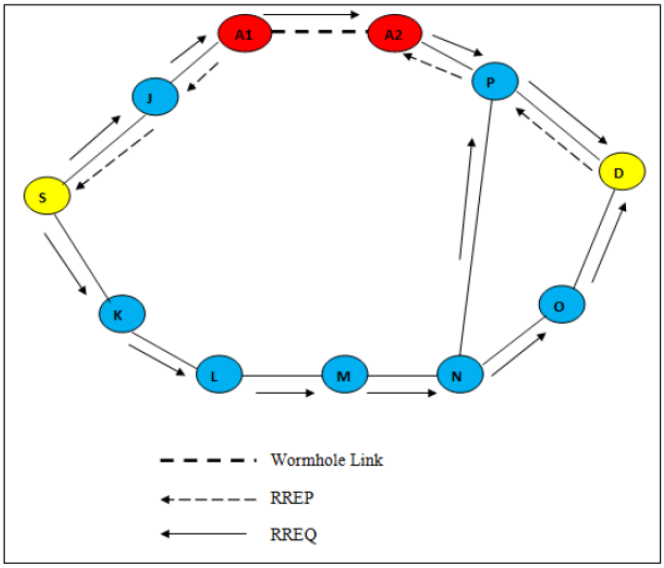

Figure 2 Wormhole Attack

In this, link is established between colluding node for sending data packet and it could be established via wired

link or wireless link between two colluding attacker and create a illusion that they are one hope neighbour but in reality they are not neighbour. When node transfer a data via wormhole link than attacker are able to gain the confidential information, or drop the packet [13]. Above figure shows an example of the wormhole. In the figure, A1 and A2 are two attackers that are connected by high speed channel. When source S wand to send a packet to destination D than it send a RREQ packet for finding a route between source to destination, According to figure 2, S send a RREQ packet to its immediate neighbors J and K, J and K receive a packet and send it to their neighbors. And node A1 which is the neighbor of J when Received the RREQ packet than it send a RREQ packet to the colluding node A2 via high speed channel, A2 rebroadcast the RREQ to its neighbor P, request which passes through a wormhole link reach at destination first because colluding node are connected through high speed channel. So D will choose route and send a RREP via a path D-P-J-S and ignore the other RREQ that arrive later. Then S sends a data packet via a path S-J-P-D to destination D [14].

B. Black-hole Attack

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks [15].

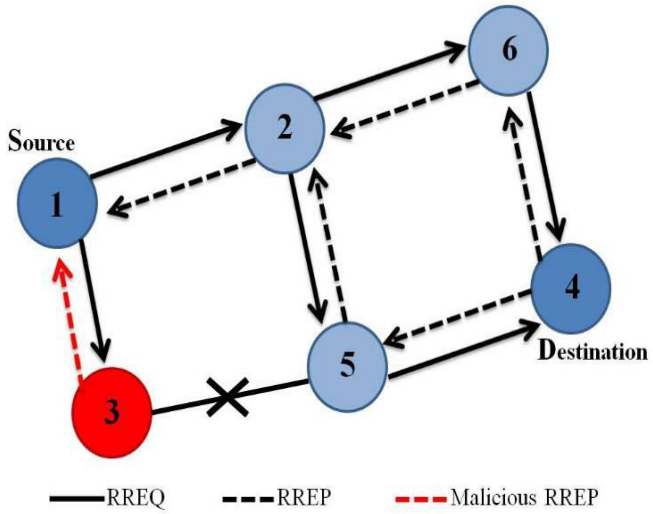

Figure 3: Black-hole Attack

An example is shown as Figure 3, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely.

IVProposed Work

A.Problem Formulation

Internet security is a fashionable and fast-moving field; the attacks that are catching the headlines can change significantly from one to next. Regardless of whether they're directly relevant to the work you do, network-based attacks are so high-profile that they are likely to have some impact, even if you only use hacker stories to get your client to allocate increased budgets to counter the more serious threats. By analyzing and summarized base existing concept that we come to the basic limitation/problem in this-
In networking devices, transmission of data between sources and destinations being happened through routing option.

When network functionalities is discover communication path, this path can adopt new nodes and can leave previous nodes.

So, in this scenario a malicious node can also join the network and harm the basic functioning of the networks. Therefore, security is key essential point for secure path between source and destination is required to build up.

The Problem in [16] is issuing "additional control messages", means that there is need to maintain trust table for every performance that is forming Routing excessive overhead which can affect the different network parameters.

Consequently, degrading the overall network performance that causes inversely proportional to the network disruption.

B. Suggested Solution

The suggested solution needs to develop an approach by which the routing algorithm self-detect and prevent both

network based malicious attack in MANET. Therefore the proposed Trust based approach needs to incorporate the following solution.

There various security issues are in the MANET network due to their ad hoc nature. Additionally the system already faces the problem related to performance issues due to mobility and routers capability. When the security attackers are formed in network the network performances are rapidly degraded. Due to routing nature the main two issues are arises Wormhole and black hole, thus required an advance security policy or architecture that helps to detect and prevent the security gap. Working with all attacks and finding the way to prevent the attacks in other words the improvement in security with all the attacks are quite complex and expensive task. Thus we include the following solution to achieve as solution for above problem.

Implement a MANET network with a Black hole attack and Wormhole attack.

Study the performance of network after attack formation

Implement detection and prevention scheme for black hole attack and Wormhole attack

Conclude the results with the performance improvement in MANET.

In this work, we will improve the Detection rate of the attack at the same time when packets are forwarded from source to destination followed by AODV routing in MANETs. The enhancement will be based on the trusted value of the threshold. In this work, development of the proposed technique will be done to increase its effectiveness in terms of energy, end to end delay, throughput and PDR.

V Conclusion

MANETs require a reliable, efficient, and scalable most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. The mobile ad hoc network is one of the most popular network technologies now in these days. In recent years the widespread availability of wireless communications, mobile computing and handheld devices has led to the growth and significance of wireless mobile ad hoc networks. Though there have been many works in the recent years on secure routing protocols. This survey paper initiate key defense against network attack i.e. black-hole and wormhole in MANET and also explore initial trust based approach, and how these solutions are capable to safe the network So the finally, by evaluate the pros and cons of obtainable techniques the open research challenges in mobile ad-hoc network are studied.

References

[1] Indrani Das and D. K Lobiyal, “Effect of Mobility Models on the Performance of Multipath Routing Protocol in MANET”, Computer Science & Information Technology (CS & IT) Computer Science Conference Proceedings (CSCP), PP. 149–155, 2014

[2] AsisNasipuri Chapter 3 Mobile Ad Hoc Networks Handbook of RF and Wireless Technologies, Newnes is an imprint of Elsevier. 200 Wheeler Road, Burlington, MA 01803, USA, 2004

[3] MousumiSardar and KoushikMajumder, “A Comparative Study on Different Trust Based Routing Schemes in MANET”, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 5, October 2013

[4] Poonam Gera, KumkumGarg and ManojMisra, “Trust-based Multi-Path Routing for Enhancing Data Security in MANETs”, International Journal of Network Security, Volume 16, No.2, PP.102-111, March 2014

[5] Kamini Singh and Gyan Singh, “A Trust based Approach for Detection and Prevention of Wormhole Attack in MANET”, International Journal of Computer Applications (IJCA) Volume 94 – No.20, May 2014

[6] Priyanka Donga and Shraddha Joshi, “A Review on Trust Based Method to Detect Black Hole Attack in MANET”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 6, June 2016.

[7] Mahamuni, K., and C. Chandrasekar. "Trusty DSR Protocol for MANET to Mitigate BLACKHOLE Attacks", International Journal of Applied Engineering Research 11.5 (2016): 3083-3091.

[8] N. Bhalaji and Dr. A. Shanmugam, “Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET”, Journal of Advances in Information Technology, Vol. 2, No. 2, May 2011

[9] Devendra Singh Kushwaha and Ashish Khare, “Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET”, International Journal of Computer Applications (IJCA) Volume 62– No.7, January 2013

[10] Vandana, C. P., and A. Francis SaviourDevaraj, "Evaluation of impact of wormhole attack on AODV", International Journal of Advanced Networking and Applications 4.4 (2013): 1652.

[11] N. Song, L. Quin, and X. Li., "Wormhole Attack Detection in Wireless Ad hoc Networks: A Statistical Analysis Approach", In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, pp. 8-15, 2005

[12] Gaurav Garg, SakshiKaushal and Akashdeep Sharma "Comprehensive study on MANETs network layer attacks," Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on IEEE 2013, PP. 1-8

[13] Yudhvir Singh, AvniKhatkar, Prabha Rani, Deepika, and DheerDhwaj Barak "Wormhole Attack Avoidance Technique in Mobile Ad-hoc Networks", Third International Conference on Advanced Computing & Communication Technologies, PP. 283-287, 2013.

[14] Viren Mahajan, MaitreyaNatu, and AdarshpalSethi, "Analysis of Wormhole Intrusion Attacks in MANETs, IEEE, 2008.

[15] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 1.1, Springer, 2011.

[16]Arya, Neeraj, Upendra Singh, and Sushma Singh. "Detecting and avoiding of worm hole attack and collaborative black-hole attack on MANET using trusted AODV routing algorithm", Computer, Communication and Control (IC4), 2015 International Conference on, IEEE, 2015