Performance Enhancement of Black-Hole Attack in MANETs

Minoti Puray, Patel College of Science and Technology, Indore, India

Priyanka Palod, Patel College of Science and Technology, Indore, India

ABSTRACT

Wireless networks are playing important role for development and ease of use of human society. It also gets a lot of attention from research community towards the betterment of applications. A wide range of applications make it very popular and backbone of technology system i.e. GSM, Bluetooth, Wi-Fi etc. In order to categorization of applications, this network gives a unique range for monitoring and surveillance. MANETs may be ad-hoc is fixed natured use to deploy into remote areas for sensing and processing desire information.

Due to distributed and open natured of wireless networks, it is vulnerable and prone for attacked to intercept and hijack network communication. Its deployment in remote areas requires more concern of security issues. Open natured communication be a magnet for attacker to intercept and catch the sensed information. Numerous security threats can adversely affect its functioning & degrade network performance. The problem becomes more critical when it deploy for defense mission.

Arbitrary network failure or node failure is the natural phenomena and may vary as per real life deployment, but intentional failure or compromising network may lead to leak the information. A various security threats like Worm-hole attack, Black-hole Attack, Gray-hole attack, Sybil Attack etc. are used for packet dropping, capturing and degrading network performance. Security in mobile networks is a challenging task. Furthermore, low profile observes that, security threats not only capture the packets but also degrade network performance. To overcome vulnerability problems, work considers blackhole attack as study target and will derive mechanism to identify and prevent mobile networks from security threat. A blackhole attack is very popular and applies on network layer by targeting vulnerabilities of routing protocols. The complete works consider Ad-hoc On Demand Routing protocol and identify several vulnerabilities.

Keywords: MANET, AODV, Blackhole Attack

1. INTRODUCTION

A mobile ad hoc network (MANET) is a group of devices or nodes that transmit across a wireless communication medium mainly based on radio frequency without any fixed infrastructure or centralized control. Cooperation of nodes is important to forward packets on behalf of every different once other destinations are out of their direct wireless transmission vary. There will be no centralized control or network infrastructure for a MANET to be set up, thus making its deployment quick and inexpensive. The nodes facility to move generously ensures a flexible and handy vibrant network topology which is another important feature of a MANET [2]. Some of the MANET applications includes emergency disaster relief, military operations over a battlefield (vulnerable infrastructure), and wilderness expeditions (transient networks), and community

ISSN: 2278 – 1323

networking through health monitoring using medical sensor network (MSN).

Every node in an ad hoc network must be willing to forward packets for other nodes. Figure1.1 shows the representation of MANET If node A want to send data to D then it is necessary A, B, C, D all are in radio range after that communication is possible among these nodes. Every node acts both as a host and as a router for the topology of ad hoc networks varies with time as nodes move, join or leave the network, with this topological insecurity requires a routing protocol to run on each node to create and maintain routes among the nodes. Mobile ad-hoc networks can be deployed in areas where a wired network infrastructure may be undesirable due to reasons such as cost or convenience. This can be quickly deployed to support emergency requirements, instant needs and coverage in emergent areas.

Security is a primary need of the real time scenarios based on wireless networks. The basic assumption of this study is that mobile nodes are normal and non-malicious nodes in the network deployment. Mobile nodes have low transmission power range due to this nodes are deployed in the transmission range of its neighbor nodes. All mobile nodes deployed in the networks are static means there is no mobility in the node. This study is based on the routing attack called blackhole attack, so all nodes in the networks are fully functional device (FFD). The results of this study are measured at different scenarios which consist less number of nodes.

2. RELATED WORK

K. Win presented a security imitation based on trust evaluation of nodes and neighbor monitoring. In this security model, sensor nodes go into immoral mode after sending packet to neighbors. Subsequently, they observe the transmission status of RREQ packets. To analyze the correlation among packets sent and that which is dropped association coefficient has been made use of. The correlation coefficient is calculated for all the neighbors and the trust factor of a node is constructed. The vector containing trust values of each of its neighbors is known as trust vector of a node. It is straightforward to detect the blackhole if the trust information available through neighbor monitoring. During the routing stage the algorithm for detection of blackhole is run.

A. Vani and D. Rao proposed a technique that combines three methods based on hop count, neighbor list count and result anomaly methods. In hop count based method the distinction between the numbers of hops of the two routes is calculated first and if the distinction is better than a certain value called the threshold value, the sender gets noticed that a blackhole exists. In Neighbor List Based Detection method secure neighbor discovery from source to destination is obtained by neighbor list and its absurdity is detected if attack is present. In variance detection, adjoining nodes of a blackhole node notices that the blackhole node has huge capacity of competition in path discovery.

Z. Alishahi et al. proposed a technique to offer security for routing packets where the malevolent node acts as a black-hole and drops packets. In this method, to make

ISSN: 2278 – 1323

accurate decisions the collaboration of a group of nodes is used.

A self-assured RREQ or RREP packet in each hop is checked in the proposed model strength of intermediate node. It allow source for trusted route option to its destination. This technique increases overhead as the node that is forwarding RREQ or RREP packets need to acknowledge the intermediate node.

3. AODV ROUTING PROTOCOLS

Routing protocols identify how routers communicate with each other, disseminating in sequence that enables them to decide on routes between any two nodes on a computer network. Routing algorithms settle on the specific choice of route. Each router has a priori information only of networks attached to it straight.

A routing etiquette shares this information first amongst immediate neighbors, and then right through the network. This way, routers gain acquaintance of the topology of the set-up.

There is Classification of routing protocols that are implemented in Wireless Sensor Network for secure routing.

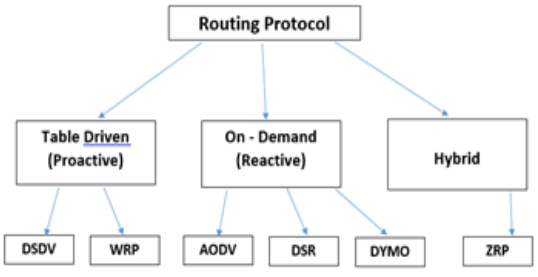

Figure 1: Classification of routing protocols

AODV is a reactive routing protocol designed for ad hoc wireless networks. In AODV routes to connect two nodes are obtained only when it is required i.e. on demand. AODV routing algorithm is especially suited for dynamic self-configured networks like MANET. AODV provides loop free routes along with route management for broken links. Bandwidth requirement of mobile nodes in AODV is comparatively less than other protocols as AODV does not require periodic route advertisements [1].

AODV uses symmetric links between communicating nodes. Nodes which are communicating or intermediate nodes on active route only maintain routing information. Nodes which do lie on active path need not maintain routing information and does not exchange routing table periodically. Furthermore, routes are discovered and maintained between two nodes only when they need to communicate or if they are acting as the intermediate node supporting in communication.

The AODV algorithm's primary objectives are as follows:

1. Initiate route discovery only when necessary.
2. Periodic exchanges utilized only for local connectivity management and not for general topology maintenance.
3. Sharing the local connectivity information with only those neighboring nodes which may need the information.

For route discovery AODV uses broadcast mechanism [41]. Instead of using source routing, routing strategy used in

ISSN: 2278 – 1323

AODV is to establish route entries dynamically at intermediate nodes. This kind of routing serves networks with large number of nodes by saving overhead required by source routes in each data packet.

Similar to DSDV, a destination sequence number is used. Each node keeps an increasing sequence number to ensure freshness of routes.

4. BLACKHOLE ATTACK

In the blackhole attack, a malicious node uncovers the messages it receives at one end of the network over a separate low-recess channel. Then it repeats messages at a dissimilar point in the sensor network. For example, when a source node is passing on data to an objective node then there can be a malevolent node in between them which selectively forwards the data packets. The blackhole attacks typically connects two unlike and far-away malicious nodes plotting to diminish their distance from each other by replaying packets next to an out-of-reach channel which is only accessible to the attacker.

A typical blackhole attack requires two or more attackers (malicious nodes) having better communication capability and resources than other sensor nodes. The attacker creates a low-latency link (high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes take up this tunnel for their communication. The strange factor is, all data packet moves from this tunnel and attacker may collect or drop data packet respectively.

5. PROBLEM INVESTIGATION

Although, energy utilization and resource consumption are major problems with MANET, but security also becomes a key prerequisite for modern age applications. Weak security or absence of security may not only conciliate classified information but also makes them accessible for malicious attacks. In the MANETs, several anomalies can occur due to their lack of processing and communicating capability, limited storage capacity, range, bandwidth and energy. These networks are usually deployed in remote area and left unattended; they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes.

One of the major issues with wireless mobile networks is to uphold confidentiality. A wireless mobile network should not leak out any of its credential even when mobiles are read by their neighbor nodes. They use encryption algorithms for privacy conservation. Encryption mechanisms are very awkward in nature as they generate security overhead and enlarge packet size for that reason. They also increase energy utilization due to encryption and decryption procedures

ISSN: 2278 – 1323

and network traffic. Finally, work concludes that, there is a necessity to find out different vibrant featured confidentiality approach based on network traffic condition and security level of current event and intermediate node for different applications.

The major security issue with wireless mobile network is insecure routing. Even though, a large amount of work has been done in this area but all the proposed techniques are based on stationary strategies. They do not consist of current network traffic, security factor of midway nodes and selected route. Further, the susceptibility of routing process gives opening to attackers for compromising mobile nodes or intermediate messages to misguide routing process or bring network into endless state. One of the major draw backs of insecure routing is increased routing time, unnecessary energy utilization, resource consumption and restricted access conditions during communication.

Wireless Mobile Networks are vulnerable to various types of attacks. These attacks are mainly: Attacks on secrecy and authentication (outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets), Attacks on network availability (attacks on availability of WSN are often referred to as denial-of-service (DoS) attacks), Stealthy attack against service integrity (the goal of the attacker is to make the network accept a false data value).

Once a node is captured by an attacker, attacker collects all the credentials such as keys and identity etc. The attacker can re-program it and replicate the node in order to eavesdrop the transmitted messages or compromise the functionality of the network. Identity attackers lead to two types attack: clone and Sybil. In particularly a harmful attack against mobile networks where one or more node(s) illegitimately claims an identity as replicas is known as the Node Replication attack. The replication attack can be exceedingly injurious to many important functions of the mobile network such as routing, resource allocation, misbehavior detection, etc.

Different kinds of holes can form in such network creating geographically correlated problem area such as coverage holes, routing holes, jamming holes, sink/black holes and worm holes, etc.

SOLUTION DOMAIN

In this section the proposed mechanism for defending against black hole attack is presented. The mechanism modifies the AODV protocol by introducing three concepts,

i. Broadcast Hello packet,

ii. Suspicious Node Detection

iii. Suspicious Node Prevention

Simulation of Mobile Ad-hoc Networks.

ISSN: 2278 – 1323

The complete work has been classified into three different situations which are listed below:

1. Simulation and Performance observation of MANET with Normal condition
2. Simulation and Performance observation of MANET with Blackhole Attack
3. Simulation and Performance observation of MANET with proposed Detection & Prevention Technique

RESULT OBSERVATIONS:

Kindly change the value in the results as per your project results.

The following metrics are used in this work for comparing the performance of AODV, AODV under attacks and Modified AODV routing protocols.

1. Throughput
2. Packet Delivery Ratio
3. End-to-End Delay

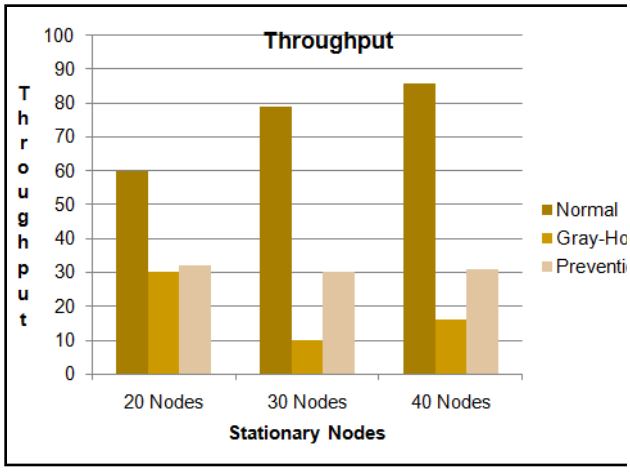

Figure 1: Throughput Analysis of Stationary Nodes

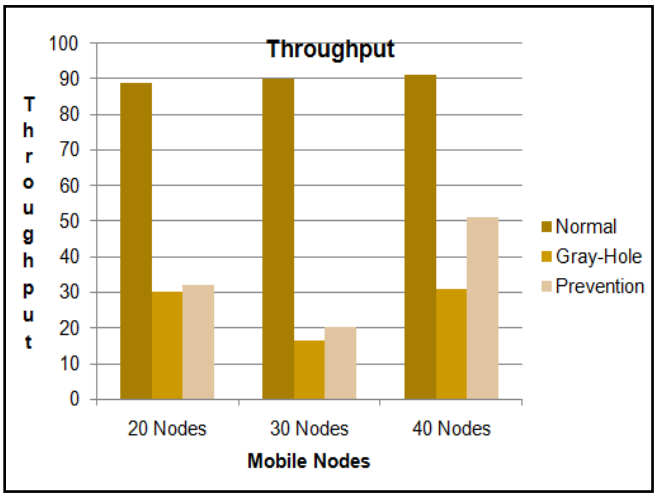

Figure 2: Throughput Analysis of Mobile Nodes

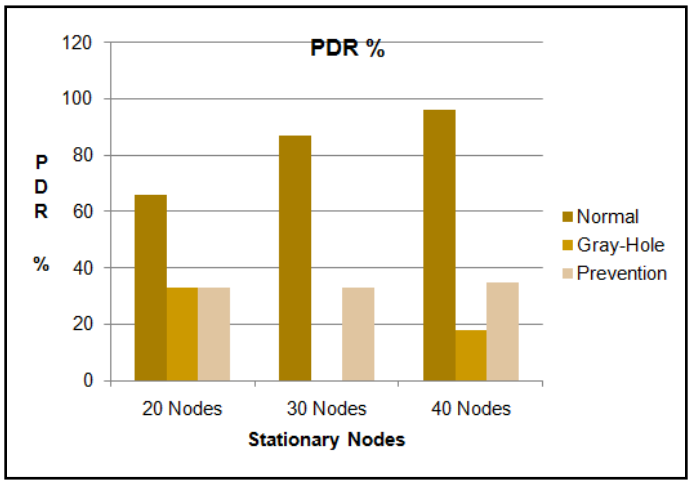

Figure 3: PDR Analysis

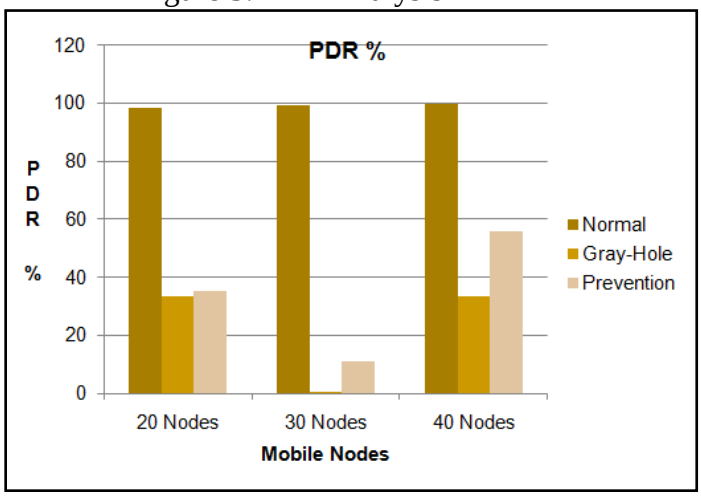

Figure 4: PDR Analysis

ISSN: 2278 – 1323

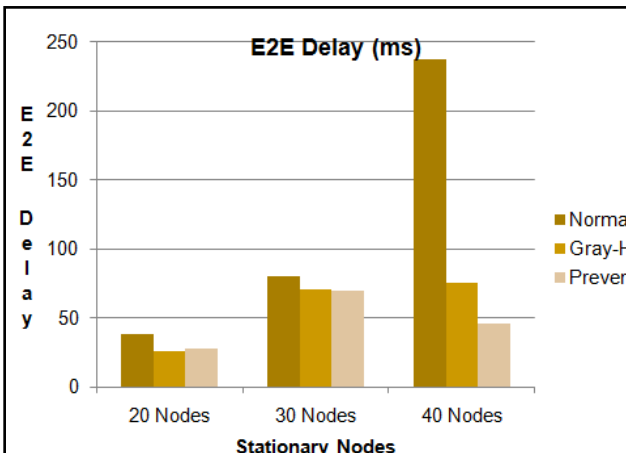

Figure 5: End-To-End Delay Analysis

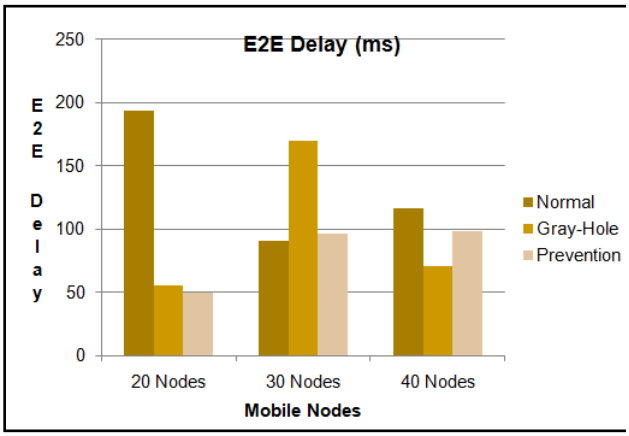

Figure 6: End-To-End Delay Analysis

6. CONCLUSION

The complete study observes that blackhole attack is one of the severe security threats in wireless networks. It not only attempts to compromise the privacy of communication but dropping of packets also degrades the network performance. The complete study generate a demand to develop a solution to detect and prevent blackhole attack in mobile ad-hoc networks.

REFERENCES

[1] Gowrishankar.S , T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "Issues in Wireless sensor networks" Proceedings of the World Congress on Engineering vol I, 2008.

[2] Pathan,A.S.K., Lee,H.W., Hong, C.S. "Security in Wireless Sensor Networks: Issues and Challenges " ICACT ISBN 89-5519-129-4, pp 1043-1048, 2006.

[3] Jaydip Sen "A Survey on Wireless Sensor Networks Security" In International Journal of Communication Networks and Information Security (IJCNIS) Vol.1, No. 2, August 2009, pp 55-74,

[4] Sangwan,A., Sindhu,D., Singh, K., "A Review of various security protocols in Wireless Sensor Network", IJCTA, ISSN:2229-6093, vol. 2 (4), july-august-2011, pp.790-797.

[5] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, Xiangke Liao "Topological Detection on Blackhole in Wireless Ad Hoc and Sensor Networks", IEEE/ACM Transaction on Networking, vol. 19, No. 6 December 2011, pp.1787-1796.

[6] Miss Morli Panday,Ashish Kr. Shriwastava, "A Review on security Issues of AODV routing protocol for MANETs", IOSR Journal of Computer Engineering(IOSR-JCE), e-ISSN:2278-0661, p-ISSN:2278-8727 vol. 14, Issue 5 (Sep. - Oct. 2013), pp.127-134.

[7] R.balakrishna, U.Rajeshwar Rao, N. Geetahanjali, "Performance issues on AODV And AOMDV for MANETs",

ISSN: 2278 – 1323

International journal of Computer Science and Information (IJCSIT), vol. 1 (2), 2010,pp. 38-43.

[8] Mohamad Y. and Alsaadi, Yi Qian "Performance Study of a Secure Routing Protocol in Wireless Mobile Ad Hoc Networks" published in proceeding of 2nd International Symposium on Wireless Pervasive Computing, 5-7 Feb. 2007, pp 425-430.'

ISSN: 2278 – 1323