International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.11, November 2015 DOI:10.15693/ijaist/2015.v4i2.26-30

Implementation of Secure Routing and Energy Efficient Mechanism for MANET

Ms. S. Soorya
P.G Student of ECE Department
P.S.R.Rengasamy college of engineering for women

Mr. G. Sivakumar
Assistant Professor of ECE Department
P.S.R.Rengasamy college of engineering for women

Dr. K. Ramasamy
Principal & Associate Professor of
P.S.R.Rengasamy college of engineering for women

***Abstract*—The adhoc networks are very much vulnerable to Dos attacks on the network layer. Black hole attack, gray hole attack are the widespread attack on adhoc networks. Here the malicious nodes interrupt data transmission in the network by transmitting false routing information. The purpose of this paper is to present an efficient Adhoc On-demand Distance Vector (AODV) protocol that removes the malicious node by isolating it, thereby ensuring secure communication. In order to achieve this goal, the intermediate nodes receiving false routing information from its neighbor node is programmed to consider that neighbor node as malicious. In adhoc network, nodes can join or leave at any time. So, an efficient security mechanism is needed. A homomorphic algorithm is used among authenticated neighbors' in the adhoc network to provide more security. To reduce the energy consumption of the nodes, data compression techniques are used.**

Index terms—MANETs AODV, LZW data compression techniques.

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks.

In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Gray hole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from.

II. MANET SECURITY AND ATTACKS

A. Black Hole Attack

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.

The method how malicious node fits in the data routes varies. Fig. 2.1 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets.

It will then send the response to node "A" before any other node. In this way node "A" will think that this is

the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

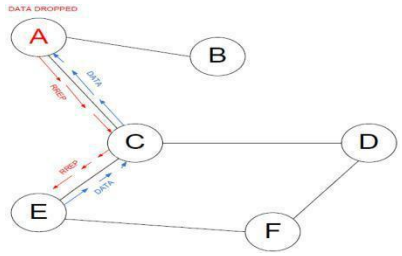

Fig 1 Black Hole Problem

B. Gray-hole attack:

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are,

- Dropping all UDP packets while forwarding TCP packets.
- Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.

Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbor, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

The gray hole attack has two phases:

Phase 1:

A malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.

Phase 2:

In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of gray hole attack is a difficult process. Normally in the gray hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack.

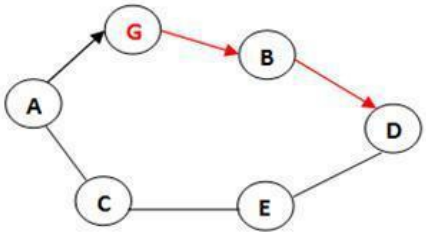

Fig 2 Gray Hole attack

III. RELATED WORK

D.M. Shila; T. Anjali [18]; proposed to investigate a serious security threat known as the selective forwarding attack (gray hole attack). In a selective forwarding attack, a malicious node refuses to forward all or a subset of the packets it receives. Such selective dropping is challenging to defend against. In this paper, we present an algorithm to defend against selective forwarding attacks based on AODV routing protocol. The first phase of the algorithm is Counter-Threshold Based and uses the detection threshold and packet counter to identify the attacks and the second phase is Query-Based and uses acknowledgment from the intermediate nodes to localize the attacker. We also present simulation results to illustrate the efficiency of the proposed algorithm. To the best of our knowledge, this is the first paper to present an algorithm for defending selective forwarding attacks in WMN. The selective forwarding attack is overcome by using the counter-threshold, detection threshold and packet counters. The wireless mesh network has unique mesh client, it waits for acknowledgement means the node can easily compromised with another.

Kozoma W, Lazos L [14], proposes a scheme REAct. REAct that provides resource-efficient accountability for node misbehavior. REAct identifies misbehaving nodes based on a series of random audits triggered upon a performance drop. We show that a source-destination pair using REAct can identify any number of independently misbehaving nodes based on behavioral proofs provided by nodes. Proofs are constructed using

Bloom filters which are storage-efficient membership structures, thus significantly reducing the communication overhead for misbehavior detection. REAct that provides resource-efficient accountability for node misbehavior. By suing the bloom filter they prove that which has a storage efficient membership. It reduces communication overhead. It increases the delay. It does not concentrate on the QOS of the network.

Detecting packet drop attacks is important for security of MANETs and current random audit based mechanism cannot detect collaborative attacks. Wang W, Bhargava B, Linder man M [16], design a hash function based method to generate node behavioral proofs that contain information from both data traffic and forwarding paths.

The new method is robust against collaborative attacks described in the paper and it introduces limited computational overhead on the intermediate nodes. We investigate the security of the proposed approach and design schemes to further reduce the overhead. Here they reduce both the detecting packet drop and collaborative attack in effective manner. It reduces the computational overhead. The complexity of the routing process. It does not give sufficient information about the routing.

Djenouri D, Badache N [19], proposed the promiscuous mode monitoring approach (watchdog (WD)) which suffers from many problems, especially when employing the power control technique. In this paper we propose a novel monitoring approach that overcomes some WD's shortcomings, and improves the efficiency in detection. To overcome false detections due to nodes mobility and channel conditions we propose a Bayesian technique for the judgment, allowing node redemption before judgment.

Finally, we suggest a social-based approach for the detection approval and isolation of guilty nodes. We analyze our solution and asses its performance by simulation. The results illustrate a large improvement of our monitoring solution in detection versus the WD, and efficiency through our judgment and isolation techniques as well. They use watch dog method for the monitoring process. So, we can easily predict the misbehaving nodes. We achieve high efficiency in the presence of number of attacks. They are not concentrates the energy factor of the network. The life time of the network is also does not increased.

IV. PROPOSED SYSTEM

A. Trust Propagation Protocol

Here the reliability manager fined the reliability of nodes. After that the trust manages find the trust of nodes and the energy will be calculated. For calculating the trust value we use the trust propagation protocol, which collects the information of neighbor nodes. By using this information we find out whether the node is trusted or not. Authentication by the trusted neighbor device. Network password-based device checking is only network authentication key. This protocol has three phases.

Phase 1: Authentication in one hop from the server.

Phase 2: Authentication in more than one hop from the server.

Phase 3: Establishment of a secure connection with another device.

B. Secure Communication

Homomorphic encryption is the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form. Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets.

The term is derived from the Greek words for "same structure." Because the data in a homomorphic encryption scheme retains the same structure, identical mathematical operations whether they are performed on encrypted or decrypted data will yield equivalent results.

C. Data Compression Techniques

Compression is useful because it helps reduce resource usage, such as data storage space or transmission capacity. Because compressed data must be decompressed to use, this extra processing imposes computational or other costs through decompression. **Lempel–Ziv–Welch** (**LZW**) is a universal lossless data compression algorithm created by Abraham Lempel, Jacob Ziv, and Terry Welch.

It is the foremost technique for general purpose data compression due to its simplicity and versatility.

Typically, you can expect LZW to compress text, executable code, and similar data files to about one-half their original size. LZW also performs well when presented with extremely redundant data files, such as tabulated numbers, computer source code, and acquired signals.

V. RESULTS

False positive rate is the ratio of number of original node detected as malicious node to the total number of original nodes.

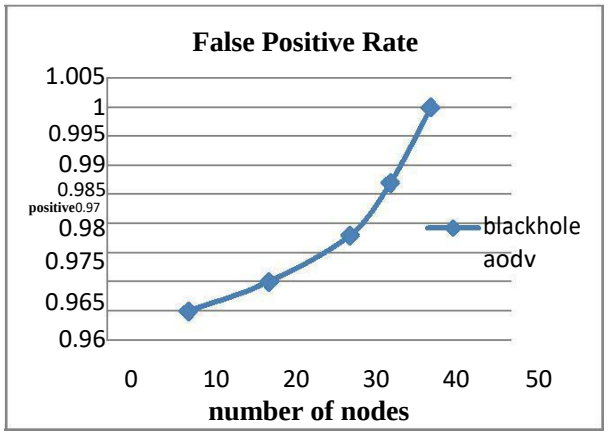

Fig 4.1 False Positive Rate

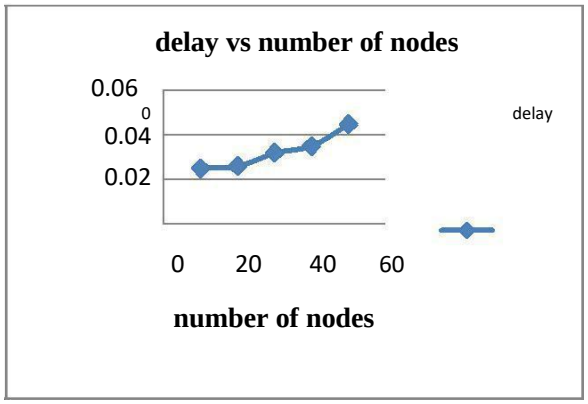

Fig 4.2 delay vs number of nodes

The graph is plotted between the number of nodes and delay. If the number of nodes increases the delay is also increased.

VI. CONCLUSION & FUTURE WORK

Among various others, the Black hole attack and Gray hole attacks are considered as the most dangerous attacks towards adhoc network. Most of the traditional methods lack reliability. Also, under these attacks, the Packet Delivery Ratio (PDR), Throughput, may decrease, as the number of malicious nodes increases. So a new mechanism for securing ad hoc networks has been proposed. Whenever a network is created using NS-2 simulator, an advanced version of AODV is applied first to remove the malicious nodes causing Black hole attack & gray hole attack. Further Homomorphic encryption algorithm is applied before transmitting data packets. In conclusion, as a result of all these mechanisms, Black hole attacks can be prevented and specifically worthy of attention is the proven increase in throughput and increased Packet Delivery Ratio.

REFERENCES

[1] Ming-Yang Su," Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detectionsystems",ComputerCommunications 34,ELSEVIER 2012.

[2] Sisily Sibichen, Sreela Sreedhar,"An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks", ISBN: 978-1-4673-5150-8, IEEE 2013.

[3] shashi gurung, aditya kumar, krishan kumar saluja,"survey of black hole attack detection in mobile adhoc networks", International Joint Conference, 7th July 2013, Goa, India, ISBN: 978-81-927147-7-6.

[4] Chanchal Aghi, Chander Diwaker, " Black hole attack in AODV routing protocol: A Review " , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 4, April 2013 .

[5] A. Baadache and A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks" ,IEEE communications surveys & tutorials,2013.

[6] V. Shanmuganathan, T. Anand," A Survey on Gray Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012.

[7] Rutvij H.Jhaveri, Sankita J. Patel2 and Devesh C. Jinwala, "Novel Approach for Gray Hole and Black Hole

Attacks in Mobile Ad-hoc Networks", 2012 Second International Conference on Advanced Computing & Communication Technologies.

[8] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda, " Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method", International Journal of Emerging Technology and Advanced Engineering , Volume 2, Issue 1, January 2012.

[9] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, " Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea,pp.755-760, Feb. 13-16, 2011.

[10] Fan-Hsun Tseng, Li-der chou and Han-chieh chao, "A survey of black hole attack in wireless mobile adhoc networks", springer journal 2011.

[11] Vishnu KA, Paul J "Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks"InternationalJournalofComputer Applications 1(22):38–42. doi: 10.5120/445-679,2010.

[12] Y.F. Alem and Z.C. Xuan. ," Preventing black hole attack in mobile ad-hoc networks using anomaly detection", IEEE International Conference on, volume 3, pages V3– 672., 2010.

[13] Raj PN, Swadas PB "DPRAODV: A Dynamic Learning System Against Black hole Attack in AODV based MANET" International Journal of Computer Science vol.2,2009.

[14] Kozma W, Lazos L "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits" Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009.

[15] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato " A dynamic anomaly detection scheme for aodv- based mobile ad hoc network", IEEE Transactions on Vehicular Technology, VOL. 58,NO.5 2481, june 2009.

[16] Wang W, Bhargava B, Linder man M, "Defending against Collaborative Packet Drop Attacks on MANETs", 2nd International workshop on Dependable Network Computing and Mobile Systems, 27 September 2009.

[17] D.M. Shila; T. Anjali; "Defending selective forwarding attacks in WMNs, IEEE International Conference on Electro/Information Technology", 96-101, 2008.

[18] Djenouri D, Badache N, " Struggling Against Selfishness and Black Hole Attacks in MANETs", Wireless Communication and Mobile Computing Vol. 8 Issue 6, pp 689-704, August 2008.

[19] Yu CW, Wu T-K, Cheng RH, Chang SC (2007) "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", Paper presented at the PAKDD workshops, Nanjing, China, Springer-Verlag Berlin Heidelberg 2007.

[20] Gao Xiaopeng Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", IFIP International Conference on Network and Parallel Computing, 2007.

[21] Al-Shurman M, Yoo S-M, Park S ,"Black Hole Attack in Mobile Ad Hoc Networks". Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[22] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.