Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Zone and Backzone Formation Algorithm to Improve Security in Mobile Adhoc Network

[1]Dr. K. Maheswari, [2]P. Lokana
Associate Professor, Department of Computer Application, SNR Sons College, Coimbatore, India
Assistant Professor, Department of Computer Science, Dr.SNS Rajalakshmi College of Arts & Science, Coimbatore, India

Abstract— With the increase in use of MANETS, security has become an essential requirement to provide protected communication between mobile nodes. To overcome the challenges, there is a need to build a multifence security solution that achieves both broad protection and desirable network performance. MANETs are vulnerable to various attacks. The proposed system has to detect and prevent black hole and Flooding attacks. Black hole is one of the possible attacks. Black hole is a type of routing attack where a malicious node advertises itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node. It can be used as a denial-of-service attack where it can drop the packets later. A novel method is designed to detect black hole attack: ACO, which isolates that malicious node from the network. To complement the reactive system for every node on the network. This agent stores the Destination sequence number of incoming route reply packets in the routing table and calculates the threshold value to evaluate the dynamic training data in every time interval. This solution makes the participating nodes realize that, one of their neighbours is malicious; the node thereafter is not allowed to participate in packet forwarding operation.

Intentional flooding may lead to disturbances in the networking operation. This kind of attack consumes battery power, storage space and bandwidth. Flooding the excessive number of packets may degrade the performance of the network. This study considers hello flooding attack. As the hello packets are continuously flooded by the malicious node, the neighbour node is not able to process other packets. The functioning of the legitimate node is diverted and destroys the networking operation. Absence of hello packet during the periodical hello interval may lead to wrong assumption that the neighbour node has moved away. So one of the intermediate neighbour nodes sends Route Error (RERR) message and the source node reinitiates the route discovery process. In a random fashion the hello interval values are changed and convey this information to other nodes in the network in a secured manner.

Finally, in previous work presents ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. Zoning and backbone formation are widely used techniques to manage the routing operation in mobile ad hoc networks (MANETs). In this work, the algorithms are provided to form a backbone that is highly resilient to mobility and topology variations in mobile ad hoc networks. The first algorithm forms zone of nodes in the mobile network each with a random forwarder. The zones are constructed in a balanced way to distribute the network load evenly. The second algorithm builds a ring network among the random forwarder of the zones. The ring backbone is constructed in a fault tolerant and energy efficient way. These two algorithms are integrated in communication architecture. To the best of the knowledge, the algorithms are the first attempts that construct balanced zones with a ring backbone. To show the operation of the algorithms, analyze their proof of correctness, time and message complexities and provide the simulation results in ns2 environment against the density, number of zones and mobility of the network. The proposed algorithms are compared with the existing algorithms and show that the algorithms create controllable number of balanced zones and robust ring backbone infrastructures while providing low message count and run-time.

Keywords— Blackhole attack, Flooding attack, ACO and Backbone Formation.

I. INTRODUCTION

Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. “Identity and location anonymity of sources and destinations” means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations. For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route. Also, in order to dissociate the relationship between source and destination (i.e., relationship unobservability), it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, an Anonymous Location-based and Efficient Routing protocol (ALERT) are presented. ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to send the data to the relay node. In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks.

But some of the active attacks are not detected in the mobile adhoc networks. Black hole is one of the possible attacks. Black hole is a type of routing attack where a malicious node advertises itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node. It can be used as a denial-of-service attack where it can drop the packets later. Another attack is called flooding attack. Flooding is a type of Denial of Service (DoS) attack in MANET. Intentional flooding may lead to disturbances in the networking operation. This kind of attack consumes battery power, storage space and bandwidth. Flooding the excessive number of packets may degrade the performance of the network. This study considers hello flooding attack. As the hello packets are continuously flooded by the malicious node, the neighbour node is not able to process other packets. The functioning of the legitimate node is diverted and destroys the networking operation. Absence of hello packet during the periodical hello interval may lead to wrong assumption that the neighbour node has moved away. So one of the intermediate neighbour nodes sends Route Error (RERR) message and the source node reinitiates the route discovery process. In a random fashion the hello interval values are changed and convey this information to other nodes in the network in a secured manner. So, in the proposed system a novel method is used to detect the black hole and flooding attack.

The objective of the work is to improve routing by removing misbehaving and selfish nodes thereby increasing the security and improving the performance of Network. In order to achieve the above security goal, the misbehaving nodes and the selfish nodes are to be identified and then their presence in the tree must be made insignificant as to improve security and performance. This is made possible either by pruning away the node or by not routing any packets through that node and finding alternate ways for the child nodes of that "misbehaving nodes". The proposed system is to detect and prevent the two attacks as Black hole Attack and Flooding Attack. Zone formation and backbones using zones are provided in MANETs in order to decrease the number of messages and total time spent for routing.

II. RELATED WORKS

Preserving location in ad hoc networks[1], especially for geographic routing, appears to be quite challenging. The expected solution is not only required to prevent location sniffing from outside of the network, but also from the inside. "Good" nodes are not supposed to learn others' location because the lack of proper centralized administration in ad hoc networks enforces limited pressure of investigation and legal pursuits for information leaking. In centralized wireless networks, such as cellular networks, the problem of location exposure also exists, but typically users have a privacy agreement with their operators. User location is only collected by base stations rather than by other users. However, it is not so practical for each node to enforce privacy policies in ad hoc networks. Traditional privacy preserving approaches based on centralized control become not suitable in the context. Note that the forwarding strategy used in this work is greedy forwarding, because usually greedy forwarding has a satisfactory delivery performance even in a modest-density network. Anonymous location forwarding algorithm and greedy algorithm are proposed in this scheme by Z. Zhi and Y.K. Choong in 2005.

Securing Location Aware Services Over VANET Using Geographical Secure Path Routing by V. Pathak, D. Yao, and L. Iftode in 2008 [2] in this work, an infrastructure-free secure geographic routing protocol is presented. The geographical secure path routing (GSPR) protects adhoc routing against malicious nodes and passive adversaries. The routing protocol operates on location aware anonymous nodes to provide privacy preserving secure geographic routing for ad-hoc networks. The protocol has the following goals:

- Route messages to desired geographic locations in the presence of malicious nodes. Detect and avoid bad geographic regions containing malicious or faulty nodes.
- Authenticate self-generated public keys and geographic locations of nodes on the routing path.

To this end, a framework for Anonymous Location-Aided Routing is constructed in MANETs (ALARM) [3] by

K.E. Defrawy and G. Tsudik, in 2007 which demonstrates the feasibility of obtaining, at the same time, both strong privacy and strong security properties. By privacy properties mean node anonymity and resistance to tracking. Whereas, security properties include node/origin authentication and location integrity. Though it might seem that the security and privacy properties contradict each other, to show that some advanced – yet practical – cryptographic techniques can be used to reconcile them.It uses nodes' current locations to construct a secure MANET map(LAM format). Based on the current map, each node can decide which other nodes it wants to communicate.

First, it shows how to obtain privacy-friendly on-demand location-centric MANET routing. (By "privacy-friendly" mean resistant to node tracking by both outsider and insider adversaries) by K.E. Defrawy and G. Tsudik,in 2008[4] . Moreover, this is achieved without sacrificing security. The need for comprehensive addressing is fundamental in most networks. Some form of a unique address (or name) is usually a pre-requisite for one node to communicate with

another. However, argue that in a privacy-conscious MANET setting, using long-term or persistent identifiers can be harmful. MANET routing protocols vary widely in terms of how much topological information is made available. Link-state protocols reveal the entire topology, whereas, some distance-vector protocols provide no information beyond the hop-count and the next hop for a given destination. It uses Group signature scheme algorithm.

Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, by Y.-C. Hu, A. Perrig, and D.B. Johnson in 2005 [5] . It makes two contributions to the area of secure routing protocols for ad hoc networks. First, give a model for the types of attacks possible in such a system, and describe several new attacks on ad hoc network routing protocols. Second, the design and performance evaluation is presented of a new on-demand secure ad hoc network routing protocol, called Ariadne, that withstands node compromise and relies only on highly efficient symmetric cryptography. Ariadne can authenticate routing messages using one of three schemes: shared secret keys between all pairs of nodes, shared secret keys between communicating nodes combined with broadcast authentication, or digital signatures. To primarily discuss here the use of Ariadne with TESLA , an efficient broadcast authentication scheme that requires loose time synchronization. Using pair wise shared keys avoids the need for synchronization, but at the cost of higher key setup overhead; broadcast authentication such as TESLA also allows some additional protocol optimizations "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol, by X. Wu, in 2005[8]. This research proposes a routing algorithm, named AO2P, to achieve communication privacy in ad hoc networks. . Only the position of the destination is exposed in the network for route discovery. To discover routes with the limited routing information, a receiver contention scheme is designed for determining the next hop. Pseudo identifiers are used for data packet delivery after a route is established. Real identities (IDs) for the source nodes, the destination nodes, and the forwarding nodes in the end-to-end connections are kept private. Anonymity for a destination relies on the difficulty of matching a geographic position to a real node ID. This can be enforced by the use of secure position service systems. Node mobility enhances destination anonymity by making the match of a node ID with a position momentary.

An anonymous geographic routing algorithm by X. Wu, J. Liu, X. Hong, and E. Bertino[10] in 2008 is suggested that uses fuzzy destination positions. The notion of fuzzy position is used in privacy-preserving LBSs. Under such an approach, a mobile user intentionally provides inaccurate positions to services in order to protect its real positions. Here, use a fuzzy position in geographic forwarding (geo-forwarding) to prevent adversaries from obtaining the real position of a node and, therefore, to prevent a destination ID from being discovered based on its position. A client generates a pseudo destination (PD), which is chosen in such a way that when data packets are forwarded to the location, the real client has a high probability of receiving them. Such a position is sent to the application server, toward which the server sends packets. The successful delivery in such a routing algorithm relies on the broadcast nature of wireless communication, where a transmission can always be received by all the nodes within the transmission range of the sender.

III. PROPOSED METHODOLOGY

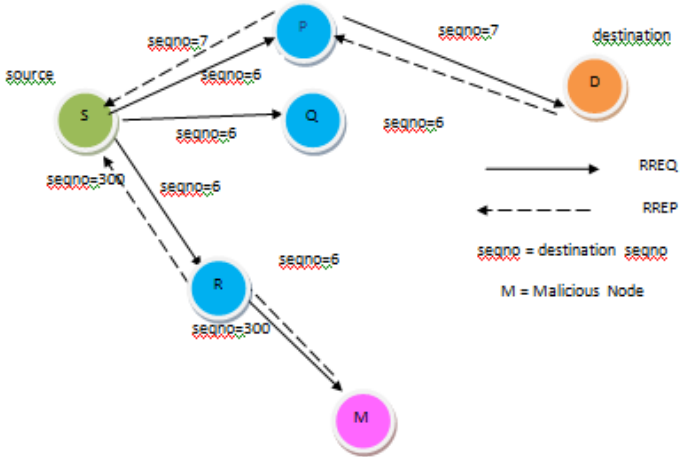
Black Hole attack

BlackHole Attack is a type of Denial-of-services (DOS) attack. This is also called Sequence Number Attack (SNA) because it is created by sequence number. Sequence number is monotonically increasing number and maintained by originator node of the RREQ and RREP message in the network. AODV routing protocol includes key features such as RREQ and RREP (For route discovery), RERR and HELLO message (For route maintenance), sequence number and hop count. AODV routing protocol has every route entry is assigned by destination sequence number in the routing table. RREQ and RREP message contains several of fields are shown in above figure 3. In BlackHole attack a malicious node receiving the RREQ message from the neighbouring node and more increase the destination sequence number and send reply message to the source node. Higher value of sequence number signifies the fresh information of the network. So source node accept route reply message from the malicious node and ignores lesser destination sequence number route reply message. Network traffic redirect through the malicious node.

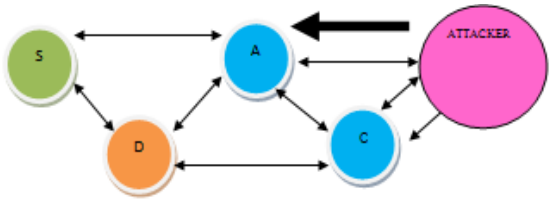
When source node S wants to send data packet to destination node D. It creates route discovery process by using RREQ message having destination sequence number suppose 6 send to neighbouring node P, Q and R. Figure 1 shows an example of BlackHole attack on AODV routing protocol. When neighbouring node receive RREQ message from source node S it updates routing table and further rebroadcast to their neighbouring nodes. Each RREQ message is uniquely identified by using RREQ Id and Source Ip address that eliminate duplicates. Route reply message (RREP) is generated by either any intermediate node having fresh route information to the destination or destination node. In figure M is a malicious node, malicious node first listen the network. It means it received RREQ message from node R and change the value of destination sequence number and assigned higher sequence number value suppose 300 in RREP message and without checking own routing table immediately sends out to its neighbouring node R towards the source node S. When destination node D generate RREP message it increases sequence number value by one and sends to neighbouring node P towards the source node S. When source node S receives multiple RREP it accepts greater sequence number RREP and ignores lesser sequence number RREP. In AODV Routing protocol higher sequence number denotes the fresh information of the network. Finally network traffic is redirected through malicious node M generated by source node S and performance of the network will be affected.

Flooding Attack

Flooding Attack can be begin by flooding the network with fake RREQ or data packet leading to the blocking of the network and reduces the probability of data transmission of the real node .



Depending upon which type of packet used to flood in the network .it is classified into three categories are HELLO FLOODING,RREQ FLOODING And DATA FLOODING. HELLO FLOODING: Some routing protocols in wireless network require nodes to broadcast hello messages to announce themselves to their neighbours. A node which receives such a message may assume that it is within a range of the sender. Some misbehaving nodes in the network flood the Hello packet continuously. Without maintaining the hello interval. It creates the disturbances in the network operation. This activity diverts the legitimate node's action in the network. Figure shows the hello flooding in the network.



RREQ FLOODING: In this type of flooding attack, the attacker broadcast many RREQ packets for the node which exist or not exist in the network. TO perform RREQ flooding the intruder disable the RREQ rate so it will effect on to consumes network Bandwidth.

DATA FLOODING: In Data flooding data packet are used to flood the network. In this flooding malicious node builds a path to all the nodes then send the large amount of fake data packet and this fake data packet fail the network resources so it will very hard to detect.

Create Network Model

A network is simulated, with minimum of 30 nodes moving in a defined area. Each node moves randomly in this area, with a speed selected in a range [0, v_{max}] with no pause time. Create a number of nodes using ns2. After the network is created various zones are formed to transmit the packets.

Detect and Prevent Balckhole Attack

In blackhole attack, the malicious node waits for the neighbours to initiate a FORWARD ANT packet. As the node receives the FORWARD ANT packet, it will immediately send a false BACKWARD ANT packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the BACKWARD ANT packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a blackhole as it swallows all objects. Node M is a malicious node which acts as a blackhol e. The attacker replies with false reply BACKWARD ANT having higher modified sequence number. So, data communication initiates from S towards M instead of D.

The BACKWARD ANT packet is accepted if it has BACKWARD_ANT_sequence number higher than the one in routing table. This solution does an addition check to find whether the BACKWARD_ANT_sequence_number is higher than the threshold value. The threshold value is dynamically updated as in every time interval. As the value of BACKWARD ANT_sequence_number is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbours. The ALARM packet has the black list node as a parameter so that, the neighbouring nodes know that BACKWARD ANT packet from the node is to be discarded. Further, if any node receives the BACKWARD ANT packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the ALARM packet. The continuous replies from the malicious node are blocked, which results in less routing overhead. Moreover, unlike ACO, if the node is found to be malicious, the routing table for that node is not updated, nor the packet is forwarded to another node.

Detect and Prevent Flooding Attack

Main objective of this study is to identify the flooder attacker and prevention mechanisms. Maintain a local connectivity is a important task. Some misbehaving nodes in the network flood the Hello packet continuously without maintaining the hello interval. It creates the disturbances in the network operation. This activity diverts the legitimate node's action in the network. In this method assumes, hello interval values are changed in a random manner. This value is encrypted and attached in the header part of the data packet. Nodes that are located in the coverage area, are able to process the header part of the packet and update this hello interval value and changing the time of sending hello packets its neighbour. But the malicious won't concentrate the processing of other packets, it continuously sends large number hello packets to its neighbour. It is unaware of these changes of hello interval.

FAA-SAODV identify and prevent from this hello flooding attack is based on their relationship with the neighbouring node. It is categorized as normal and malicious nodes. The random hello intervals are used to identify the flooder. Malicious nodes are not aware of this change of hello interval, so it does not change the interval and continuously send the packet to its neighbour. This behavior exhibits the confirmation of malicious activity and the neighbour node ignores the processing of packets.

FAA-SAODV is used to identify a malicious node based on two step process. Initially all the nodes in the network agreed to send a hello packet in a fixed interval. The first step is an analysis of the time duration of received hello packets. Node which has a variation in the fixed interval will be assumed as a normal node. Then it performs the second step for taking decision either a normal or a malicious. Calculation of allowed hello loss is also varying based on the hello interval.

Backbone formation

After zone operation is completed, zones may have no information about each other depending on the characteristics of the clustering algorithm. At this stage, independent from zone algorithm, BFA supports zones to be aware of each other. The basic idea is each zones floods *zone Info* message to network. During flooding operations, zone member nodes act as routers, by just forwarding the messages. BFA is a semi-distributed algorithm, in which each zone head collects all other's informations, executes same algorithm, and finds its next zone head on the ring. The first step of the ring formation is MST construction.

This operation is achieved by executing a central process using the collected zone head Info messages. Algorithm has two modes of operation: Hop-based backbone formation and position-based backbone formation. According to selected mode of the algorithm, *zone head Info* message can contain two types of information: hop information or position information. In hop-based backbone formation, minimum number of hops counted during flooding operation is used in MST formation. The hop information between two zone heads must be same since they must form the same MST. In highly mobile scenarios, an agreement between two zone heads must be made to guarantee the knowledge of same hop count. The other mode of operation is position-based backbone formation. In this scheme, the zone heads insert their position information in *zone head Info* message. The position information is used for central MST formation. It is obvious that hop count is a better information for MST formation, assuming the nodes are located uniformly, the position of the nodes can also be accepted as a good measure for MST formation. In position-based backbone formation there is no need for an agreement although nodes are moving. But in this mode, a position tracker like a GPS receiver or a localization technique is needed.

Performance Evaluation

Performance Metrics**:** In the simulations use several performance metrics to compare the proposed ALERT protocol with the existing one. The following metrics were considered for the comparison were

a) Throughput: Number of packets sends in per unit of time.

b) Packet delivery fraction (PDF): The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.

c) End to End delay: Measure as the average end to end latency of data packets.

d) Normalized routing load: Measured as the number of routing packets transmitted for each data packet delivered at the destination.

Black hole detection algorithm

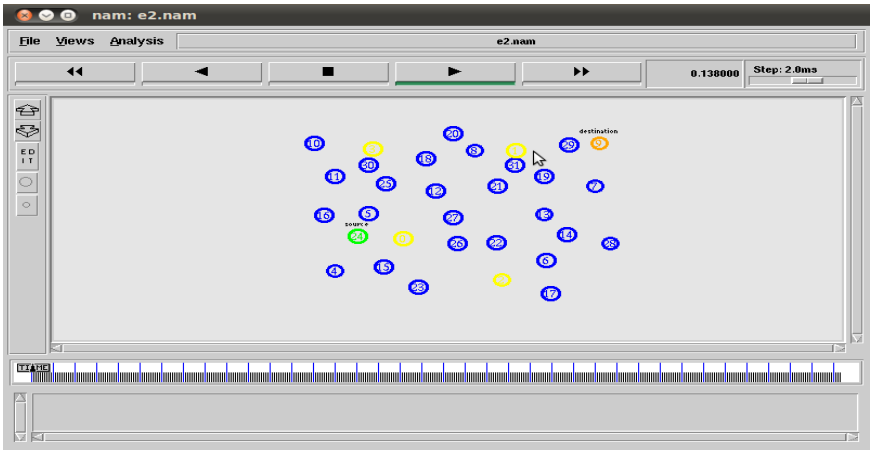
Step 1: Initialize the nodes in the network $N = n_1, n_2, \ldots n_i$
Step 2: S broadcasts FORWARD ANT packets in the network
Step 3: If n_i receives FORWARD ANT packet
Step 4: Analyze the sequence number
Step 5: n_i checks the sequence number
Step 6: If $(Seq\ no > Th)$ //Th=Threshold
Step 7: Node is suspected to malicious and adds to black list\
Step 8: Sends ALARM packet to the neighbours
Step 9: Else
Step 10: Consider as normal node
Step 11: End if
Step 12: Threshold value is updated dynamically

Flooding attack detection algorithm

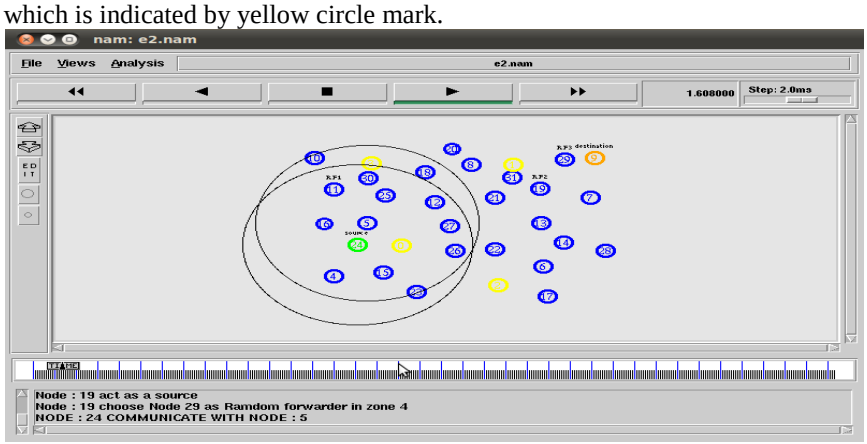
Step 1: Initialize the nodes in the network $N = n_1, n_2, \ldots n_i$
Step 2: Initiate to send hello packets to maintain local connectivity
Step 3: n_i computes the receiving time of the hello packets
Step 4: $If\,(receiving$ hello interval $< current\ random\ hello\ interval)$
Step 5: Consider as malicious node
Step 6: Else
Step 7: Consider as normal node
Step 8: End if

IV. RESULT AND DISCUSSION

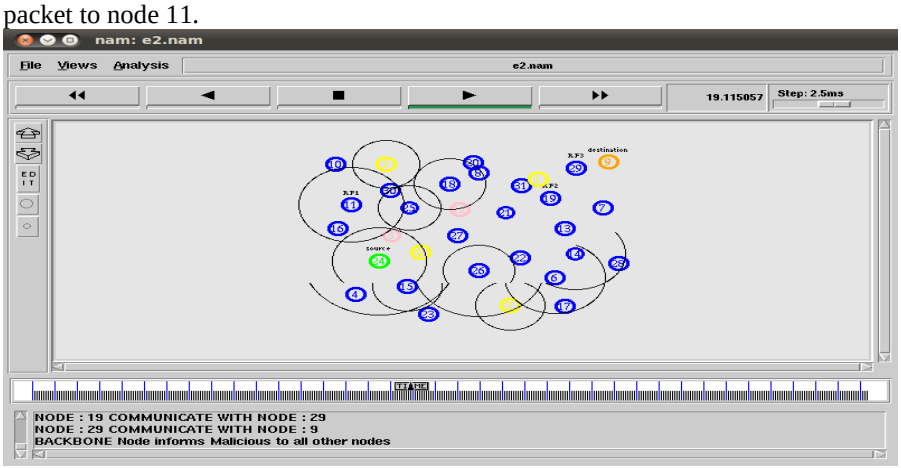
NETWORK SIMULATOR WINDOW:



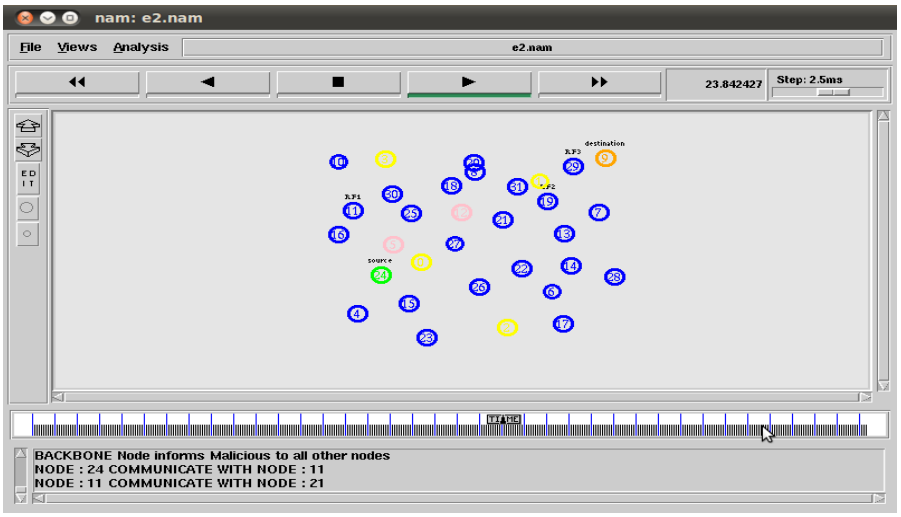
The above figure shows the Network Animator Window for the simulation of the Intilization Process. Here 24 act as a source node and 9 act as a destination node. There are 4 zones in these network window. Each zone has a backbone forwarder which is indicated by yellow circle mark.



The above figure shows the simulation result for identification of relay forwarder by source node to pass the packets. Here the source node 24 identifies the relay forwarder node 11 in zone 1 which acts source for that zone and the node 24 passes the packet to node 11.



The above figure shows the identification of blackhole & flooding attack in the network and packet transmission is stopped. After identifying the malicious node the backbone node informs malicious to all other nodes. The node 5 and 12 is malicious which is identified and blacklisted.



The above figure shows the malicious node is detected and packet passing through malicious node is prevented. It discovers the new path to transfer the packet from source to destination.

Description about network setup

In this section, the performance of the existing and the proposed system is compared. In the existing system, Anonymous Location-based Efficient Routing protocol is used. The proposed system has to detect and prevent black hole and Flooding attacks. The performance is compared for the existing and proposed method in terms of packet delivery ratio, end-to-end delay and throughput.

Input parameter,

Number of nodes

It is defined as the number of nodes in the simulation.

Description of output parameter

Packet delivery ratio

It is defined as the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$\sum$ Number of packet receive / $\sum$ Number of packet send

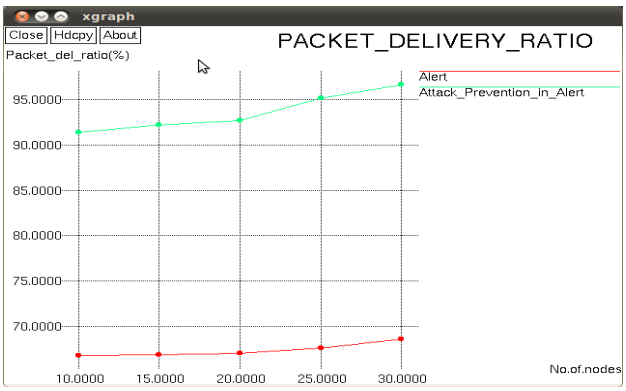
End-to-end delay

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

Throughput

Throughput or network throughput is the rate of *successful* message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link, or it can pass through a certain network node. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

Simulation Result



Packet delivery ratio

Figure Shows the simulation graph of packet delivery ratio. In the X-axis number of nodes is taken. In Y-axis packet delivery ratio is taken. In the existing system, Anonymous Location-based Efficient Routing protocol is used. The proposed system has to detect and prevent black hole and Flooding attacks. When compared to the existing method, there is high packet delivery ratio in the proposed system.

End-to-end delay

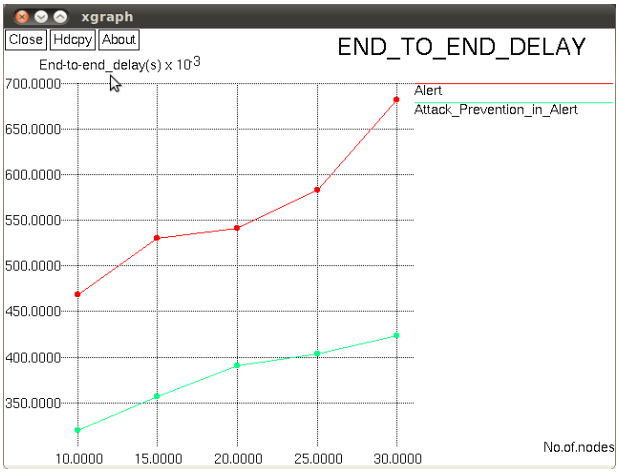


Figure Shows the end-to-end delay. In the X-axis number of nodes is taken. In Y-axis packet delivery ratio is taken. In the existing system, Anonymous Location-based Efficient Routing protocol is used. The proposed system has to detect and prevent black hole and Flooding attacks. When compared to the existing method, there is less end-to-end delay in the proposed system.

Throughput

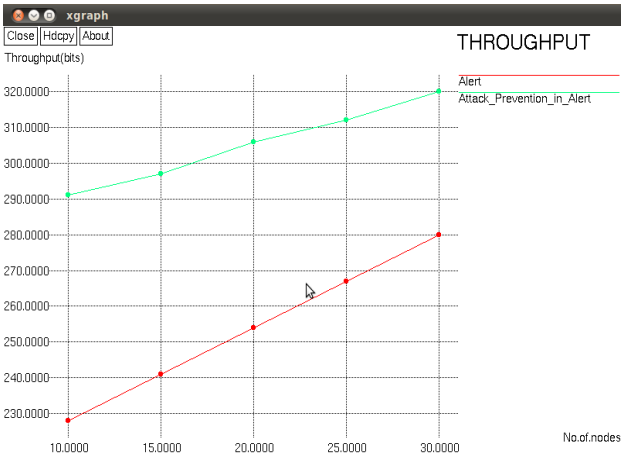


Figure Shows the throughput. In the X-axis number of nodes is taken. In Y-axis throughput is taken. In the existing system, Anonymous Location-based Efficient Routing protocol is used. The proposed system has to detect and prevent black hole and Flooding attacks. When compared to the existing method, there is high throughput in the proposed system.

Normalized Overhead

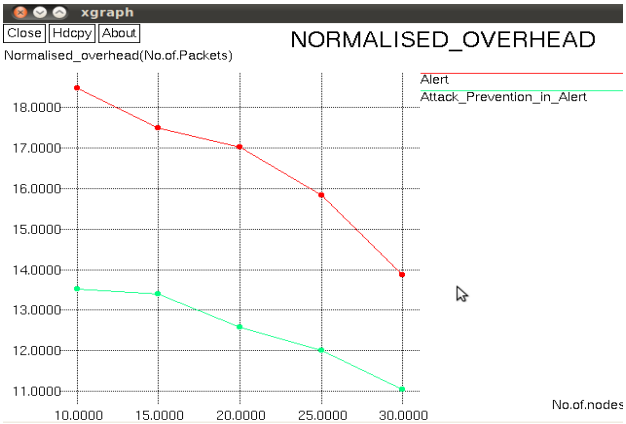


Figure Shows the normalized overhead. In the X-axis number of nodes is taken. In Y-axis normalized overhead is taken. In the existing system, Anonymous Location-based Efficient Routing protocol is used. The proposed system has to detect and prevent black hole and Flooding attacks. When compared to the existing method, there is less normalized overhead in the proposed system.

V. CONCLUSION AND FUTURE WORK

The proposed system has to detect and prevent the different types of active attacks such that black hole and flooding attack. The proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbours. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case. This system, data communication will be based on authentication, because of this it will always provide the reliable communication over the network. But still there can be risk in the authorized system, so to overcome the risk of attack, further an eligibility test is performed before the actual communication take place .In this way the proposed scheme provide security from the unauthorized nodes, no unauthorized node can start communication, it have to complete the authentication first, after that it have to pass the eligibility test. Hence, by using ACO(with threshold value factor) as a routing algorithm in MANETS, one can also be sure of not being susceptible to black hole attacks. The prevention scheme detects the malicious nodes and isolates it from the active data forwarding and routing and reacts by sending ALARM packet to its neighbours.

The second algorithm, BFA forms directed ring architecture between zone heads. BFA is not designed to construct zones; instead BFA constructs a backbone on top of a zoned network. The description is given of the algorithm with its finite state machine and algorithmic representation. To exemplified the algorithm on a sample instance. The proof of correctness, time and message complexities of BFA algorithm are analyzed. In the mobile adhoc network, there are some other attacks which degrades the network performance. So, this can be considered in future.

REFERENCES

[1] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

[2] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

[3] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.

[4] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.

[5] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.

[6] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[7] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[8] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.

[9] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.

[10] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo- Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[11] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.

[12] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), pp. 10-29, 2001.

