Impact of Security Enhancement Over Autonomous Mobile Mesh Network (AMMNET)

Rishikesh J. Teke, Manohar S. Chaudhari, Ramjee Prasad*
Department of Computer Engg. Sinhgad Institute Of Technology. Lonavala. Pune, India.
* Department of Electronic Systems CITF, Alborg University Alborg, Denmark.
rishikeshteke@gmail.com mschaudhari20@gmail.com prasad@es.aau.dk

***Abstract*— The Mobile Ad-hoc Networks (MANET) are suffering from network partitioning when there is group mobility and thus cannot efficiently provide connectivity to all nodes in the network. Autonomous Mobile Mesh Network (AMMNET) is a new class of MANET which will overcome the weakness of MANET, especially from network partitioning. However, AMMNET is vulnerable to routing attacks such as Blackhole attack in which malicious node can make itself as intragroup, intergroup or intergroup bridge router and disrupt the network. In AMMNET, To maintain connectivity, network survivability is an important aspect of reliable communication. Maintaning security is a challenge in the self organising nature of the topology.To address this weakness proposed approach measured the performance of the impact of security enhancement on AMMNET with the basis of bait detection scheme. Modified bait approach that will prevent blackhole node entering into the network and helps to maintain the reliability of the network. The proposed scheme uses the idea of Wumpus World concept from Artificial Intelligence. Modified bait scheme will prevent the blackhole attack and secures network.**

Keywords*— *Autonomous Mobile Mesh Network (AMMNET), Bait approach, Blackhole, Denial of Service (DoS), MANET, Security.

I. Introduction

Wireless Technology most popularly studied network communication technologies in recent years. MANET is one of the most transformed wireless network technologies. Autonomous Mobile Mesh Network (AMMNET) [1] is the one that is a transformation of MANET. As it is base on MANET, it is having similar properties with some additional properties. MANET is having network partitioning issue that will be overcome by AMMNET. It can adapt topology dynamically so it can use in various applications where the dynamic topology necessarily required. Autonomous Mobile Mesh Network uses a distributed client tracking algorithm [1] to track mobile nodes and maintain connectivity between them. This algorithm creates three types of the router as Intra, Inter and Free routers. In AMMNET mobile mesh node continuously monitor the mobility pattern and depends on the situation it triggers free router into one of Intragroup, Intragroup or intergroup bridge router. AMMNET consider group mobility pattern and ensures good connectivity between mobile nodes [1]. Quadra copters can also be used to deploy as free routers in the application terrain depends upon the need of the application.

Wireless mesh networks can use as backhaul network for providing Internet access [2]. AMMNET can use for communication in institutions, private residential areas and emergency services. AMMNET can also use for vast area applications such as battlefield communications crisis management that will especially have group mobility pattern.

The remainder of the paper organize as follows: Section II shows how AMMNET can be vulnerable to blackhole attack. Section III literature survey of various existing techniques. Section IV explains a brief idea of wumpus world game from artificial intelligence. Section V contains prevention of blackhole attack. In section VI, modified bait algorithm after it in section VII simulation results and finally conclusion in this paper.

II. SECURITY VULNERABILITY IN AMMNET

AMMNET is not itself providing any security measures to tackle against malicious activity. A malicious node can attack AMMNET and may damage the entire network. A malicious node can attack at the point of creation of topology that will cause severe security hole in the network. There is a different type of Denial of Service (DOS) [3] attack one of them is Blackhole attack.

A. Blackhole Attack And Its Properties

Blackhole attack is a denial of service (DoS) attack in which malicious node intend to source node that it has a valid route to the destination with a minimum hop count. Blackhole node sends fake Route Reply (RREP) message to source node having a valid route. Thus, source node chooses the path to send packets via blackhole node apparently blackhole node drops the packets without forwarding it. In this attack, the source node is unaware of the malicious node and blindly sends the packets to the malicious node. This property separates blackhole attack from rest of the other DoS attacks. Another property of blackhole attack is that one or more blackhole cooperatively makes an attack on the network and does devastating damage to the network; this blackhole attack called as cooperative blackhole attack.

B. Blackhole Attack On AMMNET

AMMNET is vulnerable to blackhole attack especially at the point of intragroup, intergroup and intergroup bridge router because these routers are the backbone of AMMNET. It is crucial to secure intra, the intergroup router as compared to mesh clients as mesh clients directly connected to the intragroup router and once security provided to the intragroup router, we automatically secure the whole group. Fig. 1 shows a case of blackhole node compromises intergroup bridge router and drops the packets.

978-1-4799-7849-6/15/$31.00 ©2015 IEEE

There are several possibilities from where blackhole node becomes a part of the network. Here consider blackhole attack on intra, inter and intergroup bridge router. One possibility is blackhole node initially as a free router, and when a group of mobile nodes are moving according to distributed client tracking algorithm, it will take place as an intragroup or intergroup router by replying false messages. Once it takes place, it will start dropping the packet and whole group or may be entire network will fall.

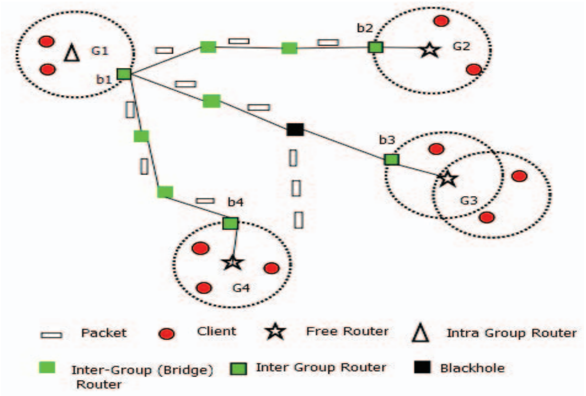


Fig. 1. A Case in which Blackhole node attacks Interbridge group router in AMMNET.

The second possibility will be. Initially, there is the absence of blackhole node and after successful of AMMNET topology blackhole enters into the network and will force to attract traffic toward itself from one of the intra or intergroup routers this leads to a serious threat to the network.

III. Related Work

Security in wireless networks is important any many of researcher worked under it. There are various kinds of countermeasures on blackhole attack some are also applicable to cooperative blackhole and greyhole attack.

J. Sen et al. [4] proposed a technique for detection of cooperative blackhole attack in a mobile ad-hoc network on AODV [5] protocol. In this technique, authors proposed a table-based data structure to detect blackhole node in the network. A table named Data Routing Information (DRI) table placed in each node in which there are two fields '*From*' and '*Through*'. *From* represents data on a routing packet from a node and *Through* represents data on routing packet through a node that results in binary values. Entry 1 for successful from the node and through the node, entry 0 for unsuccessful and vice versa. Both entries 0 represent blackhole in the network. Various modifications are carried out on DRI table especially extending these tables with more fields for enhancing the output and performance parameters. In the extended DRI table, more fields are added to track the malicious behavior of greyhole attack [6], [7].

A new scheme is Cooperative Bait Detection Scheme (CBDS) proposed by Jian-Ming Chang et al. [8], in this method authors proposed the scheme for detection and prevention of collaborative blackhole and greyhole attack. A reverse tracing technique is used in CBDS to detect and prevent malicious activity. CBDS based on DSR [9] protocol and initially detection phase is proactive, and subsequent steps are carried out on the reactive response. If packet delivery ratio goes below threshold CBDS is used to verify any malicious activity is going on in the network, and if there is such activity detected then, it will avoid malicious node and thus frees network from malicious nodes. CBDS is carried out in three steps first is initial Bait step in which source node selects id such as IP address of one of neighboring node and send to the network. The properties of blackhole and greyhole that malicious node pretends itself in RREP message that having the route to the destination. The second step is initial reverse tracing step in this step malicious node sends a false reply to the source node thus source node to identify that node as a malicious node. The third step shifted to reactive defense phase in which it will take defensive measures such as putting the malicious node in the blacklist. This scheme is strong against greyhole and blackhole but it only deployed on DSR protocol, so it has limited scope.

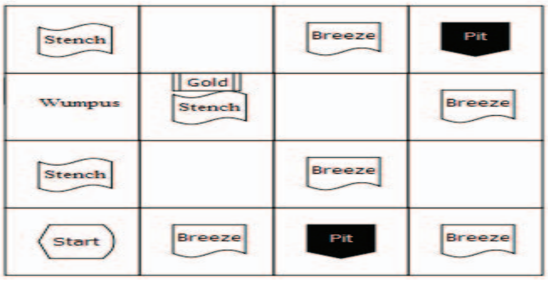
Jinyuan Sun et al. [10] proposed a security architecture called SAT for achieving anonymousness and traceability in wireless mesh network. SAT security architecture is a ticket based architecture in which there are different phases. The architecture consists of ticket distribution, deposit, fraud detection and revocation. There is a Trusted Authority (TA) which issues a ticket to the client when a client attempts to access network. A client reveals its id to trusted authority to ensure the authenticity of the client and then TA assigns the ticket to the client. The second phase is ticket deposit in this phase after acquiring ticket if the client wants to access particular service it can have it using issued valid ticket. Fraud detection used to detect fraud in tickets whether it reused, outdated ticket or multiple tickets owned by a client. Whenever one of the clients are compromised, its ticket is revoked to prevent disclosure of information. SAT architecture is well-mannered architecture for a wireless mesh network, but ticket management is a crucial and difficult task in the network.

S. Banerjee [11] proposed a technique to for detection/removal of the cooperative blackhole and greyhole attack in MANET in which total data traffic is divided into small sized blocks to detect malicious node. In this method exchange of preclude-postlude messages is carried out. The source node sends preclude message and postlude are a reply from the destination node. This technique works in two phases, first one is to detect the data loss check and second is the removal of a malicious node. At first phase on reception of postlude message node checks the data loss during transmission of packets is within threshold range if not it initiates the second phase. In the second phase is a process of detecting and removing the malicious node. The source node sends a query message to all its neighbours that include timeout period, to detect and remove a malicious node. When a timeout occurs to result in message or node is malicious message replied to the source node. Then source node will append that node in the *findmalicious* table and initialize value voting as one if it is not already there then increments by one. If that voting count exceeds, threshold value node considered as a malicious node. Thus, this method is triggered when there is actual data communication takes place. This scheme requires extra processing on source node for dividing traffic and also for processing of precluding–postlude messages. If there is network congestion, this scheme will not be efficient as there is data loss.

Yanchao Zhang et al. [12] proposed an attack resilient security architecture (ARSA) for wireless mesh networks. Architecture mainly focused on security in Routing and Medium Access Control (MAC) layer. Architecture based on id based cryptography (IBC). The architecture consists of both side authentication and key agreement in mesh client and routers. ARSA is also designed to prevent various attacks, for example, the denial-of-access attack and flooding attack. As mesh networks are future backbone of wireless broadband access technology, it requires security in all kinds of network devices such security techniques are client-router authentication, client-router key agreement, location privacy, etc. This architecture provides MAC as well as routing security for wide scale deployment of mesh networks.

IV. The Wumpus World Concept

The Wumpus world [13] is a game in which an agent had to explore a cave consists of a series of interconnected rooms. In one of the rooms in this cave, there was a wumpus that would kill the agent if it enters into the room. Some rooms contain pits and agent would die if it enters in any one of those rooms too. The goal was to find the gold that was hidden in the cave and return to the start without getting killed. There are stenches that indicate that adjacent room may contain a wumpus. The Artificial Intelligent agent will have the capacity to detect stench and accordingly make the decisions.



Stench		Breeze	Pit
Wumpus	Gold Stench		Breeze
Stench		Breeze	
Start	Breeze	Pit	Breeze

Fig. 2. A Typical Wumpus World

Fig. 2 shows a typical wumpus world game in which agent is at starting point of the cave and going to explore cave through adjacent rooms one by one. Suppose agent moves next room. Next room there will be a breeze so the agent will know that next adjacent room can contain pit so the agent will find that which room will be a safe move. Here, in this case, the agent moves to initial location and further explores new rooms one by one. Thus agent will find its way to gold.

A. Wumpus World an analogy with blackhole attack

MANET can visualize as a kind of world with the wumpus world analogy. Here Blackhole is analogous to wumpus in wumpus world and each room can be considered as nodes that are in the radio range of each other. Pits can be other malicious nodes in the MANET. Here in MANET every node acts as an agent and receives and forward packets from neighboring nodes. After detecting stench or breeze agent will decide to enter the room. In the case of MANET, a node decides to forward packets. And after detecting the blackhole node, the node will decide that which node it should forward packets so that packets will not fall.

V. Prevention of Blackhole Attack

There are various techniques to tackle blackhole attack, and some of them discussed previous sections. In this paper, bait scheme considered for detection and stench in wumpus world idea is used for prevention of blackhole attack. In the bait scheme[8] modification done as last part is sending alarm packets to neighbouring nodes. In this case possibility of threat is that what if this type of alarm messages are sent by the malicious node and neighbouring nodes will trust on these messages. Another case of notification messages is that if these messages broadcasted frequently then there is a network overhead and may cause congestion in the network. Another issue is that how neighbouring node will trust on such alarm message that there is a blackhole and should avoid bait procedure, so this is a vulnerability in the network.

To reduce such kind of overhead and vulnerability, avoid these messages. Instead, apply bait procedure from each and every node that is within its radio range, and if there is a blackhole present, then mark those nodes that are neighbours of blackhole node. If there is the message coming from a node to a neighbour of blackhole node, then it will forward the message to a different node other than blackhole node. In this way, the source can send the packet to destination packet without the involvement of blackhole node. Here nodes will not send any notification messages. We are using the concept of wumpus world problem from Artificial Intelligence.

VI. Modified Bait Scheme

In AMMNET, a source node going to send packets to the destination node if the first start with route discovery process. At the time of root discovery process, it also starts timers to check packet delivery ratio. If packet delivery ratio goes below threshold value it will do bait detection[8] but in this bait detection only bait messages exchanged, and alarm messages will not be transmitted to neighbouring nodes because these alarm messages will cause network overhead. Instead sending alarm messages node that is adjacent to blackhole node will store a flag that indicate that one of the adjacent nodes is a malicious node. Whenever source node sends packets, intermediate nodes firstly check whether the flag gets set or not if the flag is set it means that there could be a malicious node in the neighbouring node and if the flag is not set then it is secure to forward packets. If the flag set then the node will forward the packet to a node other than blackhole node that is having minimum destination sequence number[6]. This procedure repeated if packet delivery ratio falls below a threshold. The threshold value dynamically updated. Algorithm will prevent the malicious node from entering into the active path.

Procedure for detection and prevention of blackhole attack shown in following Modified bait algorithm. When a source node is going to communicate with destination node following, steps are carried out.

Algorithm 1: Modified BAIT: Cooperative detection and prevention of malicious nodes

```
Step 1: Source node starts sending route request (RREQ) packets for route discovery
Step 2: If source received route reply within time, it means destination node is a true destination, and then start forwarding data to it.
Step 3: else if the current time is greater than discovery time threshold value, then the current time is stored into T1.
Step 4: else start resending the RREQ packets, measuring another threshold value of time in T2.
Step 5: Compute the current communication Packet Delivery Ratio (PDR) performance
PDR = no_packet_recieved/no_packet_sent;
Step 6: if (PDR < threshold), sending bait RREQ
Step 7: Any nodes those sending RREP considered as a malicious node. This malicious node address added to the blacklist of malicious nodes.
Step 8: Create the alarm packet to broadcast to source neighbouring nodes and set the flags at neighbouring node. (Alarm packet contains the address of malicious node)
Step 9: If current source node does not have a new neighbor, then find a new neighbor and add them to its list excluding the malicious node. Broadcast the malicious nodes packet to all valid neighbors.
Step 10: Else neighbor list is not empty, and then send packet to all its neighbouring nodes except malicious nodes
Step 11: Update dynamic threshold value
Step 12: if (T2<T1), then
if (threshold < 0.95), then
threshold = threshold + 0.01;
else
if (threshold > 0.85), then
threshold = threshold - 0.01;
Step 13: if (Time < 800), then
return threshold;
else
threshold = 0.9;
Step 14: Stop.
```

VII. SIMULATION

An extensive simulation carried out on Network simulator-3 (NS3) [14] with AODV protocol although bait detection scheme applied to DSR protocol. Here considered scenario by varying nodes from 25 to 81 with five source-destination pairs. In simulation five malicious nodes are considered that are not cooperative with each other with considering following simulation parameters.

TABLE I. SIMULATION PARAMETERS

Simulation Parameters	
Parameter	***Value***
Application Traffic	CBR
Transmission Rate	4 packets/sec
Packet Size	64 kb
Channel Data Rate	11 mbps
Wireless Standard	IEEE 802.11
Maximum Speed	0 to 10 m/s
Pause Time	0 to 5 m/s
Number of Nodes	25 to 81
Topology	AMMNET

The simulation consists of a comparison between Grid system, AMMNET, AMMNET under Attack and AMMNET with Modified Bait [MBIAT] with considering three scenarios. In the first scenario, varying the number of nodes with constant speed and pause time. In the second scenario, keeping the number of nodes and pause time constant and vary speed and in the last scenario keeping nodes and speed constant and changed the pause time. Following are the three test cases used for simulation.

A. Varying number of Nodes:

In this scenario, by changing nodes from 25 to 81 while keeping pause time zero and speed of nodes 10m/s constant. Following results shown in case of parameters:

1. PDR:

It is the ratio of packets send by the source to packets received by the destination. Fig. 3 shows that Modified bait AMMNET shows improved PDR even presence of malicious nodes compared to the presence of malicious nodes in AMMNET. As Mbait will require more packets for detection and prevention of malicious node it shows less PDR compared to AMMNET and grid networks in which there is the absence of malicious nodes. Nature of graph shows that Mbait tends to retain its performance even though attack happened.

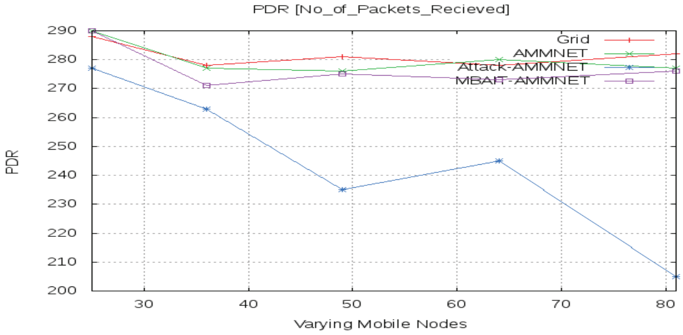


Fig. 3. PDR vs. No. of nodes with constant speed and pause time.

2. End to End Delay:

Following graph shows the comparison between grid, existing AMMNET and modified bait AMMNET. As the grid has fixed topology so delay showing in the graph is low compared to others. Also as nodes increases in the grid, there will be more connections so the delay will further reduce. Modified AMMNET will require extra bait processing for detection and prevention of malicious node so a delay of packets will happen, but it improved compared to attack happened on AMMNET.

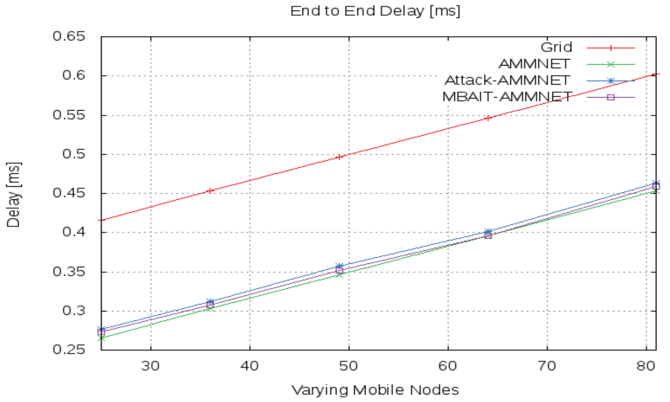


Fig. 4. End-to-End Delay vs. No. of nodes with constant speed and pause time.

3. Average Throughput:

In the grid, connections form mesh structure and packets switched from intermediate nodes. In AMMNET, there are few intermediate nodes most of them are intergroup and intragroup routers so AMMNET will give more throughput. Modified AMMNET will have fewer chances of data dropped by malicious activity, so it shows improvement in throughput compared to attack happened on AMMNET.

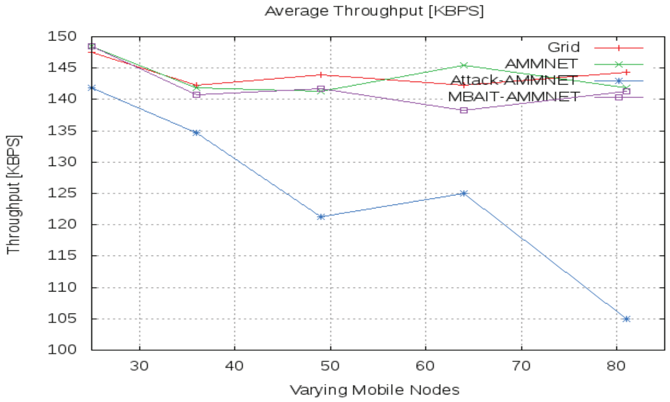


Fig. 5. Avg. Throughput vs. No. of nodes with constant speed and pause time.

B. Varying speed of nodes:

In this scenario, by changing the speed of nodes from 10 to 50m/s while keeping nodes to 25 and pause time zero constant, following results shown in case of parameters:

1. PDR:

There is considerable change in the PDR when nodes are moving faster as shown in the graph below. As nodes moving faster, PDR of AMMNET goes down because it will take the time to develop topology but regarding grid it will show steady performance. When malicious node attacks on AMMNET packet delivery ratio falls as nodes are gaining speed. Mbait shows similar deviation as of AMMNET.

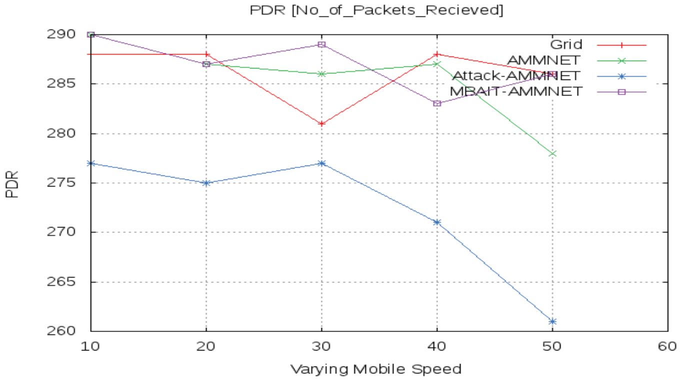


Fig. 6. PDR vs. Speed with constant no. of nodes and pause time.

2. End-to-End Delay:

Fig 7. Shows the end to end delay of packets as nodes moving at speed ranges from 10 to 50 m/s. If compared with fig 4, there is not any significant change in the delay in any of the network. It shows that as the speed of nodes gets increases delay of packets also increases exponentially.

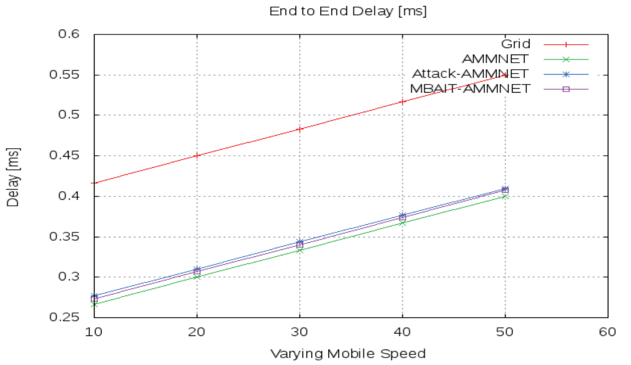


Fig. 7. End-to-End Delay vs. Speed with constant no. of nodes and pause time.

3. Average Throughput:

Throughput as shown in fig 8, increasing the speed of nodes. As increase, the speed of nodes throughput is less for all the networks. Even though Mbait AMMNET shows an increase in throughput as compared to AMMNET. As blackhole node drops, the packets throughput will decrease as nodes moving faster. At some point throughput decreases more it is because of the speed of nodes as nodes moving faster topology will change after some time and after developing topology throughput also increases.

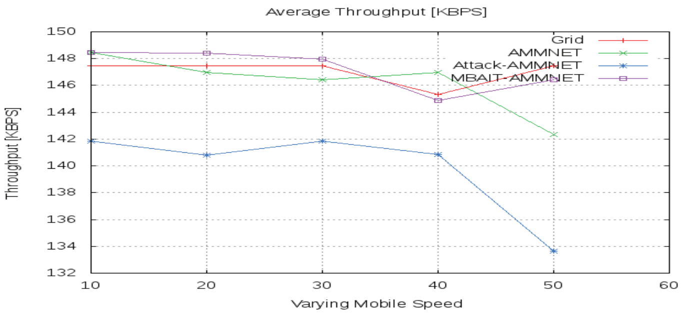


Fig. 8. Throughput vs. Speed with constant no. of nodes and pause time

C. *Varying Pause time of nodes:*

In this scenario, a pause time of nodes changed from 1 to 5 sec while keeping nodes to 25 and speed of nodes 10m/s constant. Delay almost steady even though the change in the pause time so here we avoided delay parameter. Following results shown in case of parameters:

1. PDR:

Fig 9 shows the graph under various pause times of nodes. The graph shows that as pause time increases Mbait AMMNET and AMMNET will increase the packet delivery ratio it's because of when we increase pause time it means that nodes are becoming more stable. Pause leads to topology stability and becomes more stable if pause time increases. So packet will efficiently receive by destination node that leads to increase in PDR. In the case of grid network as a grid having fixed structure there is no any change in PDR even though the change in the pause time.

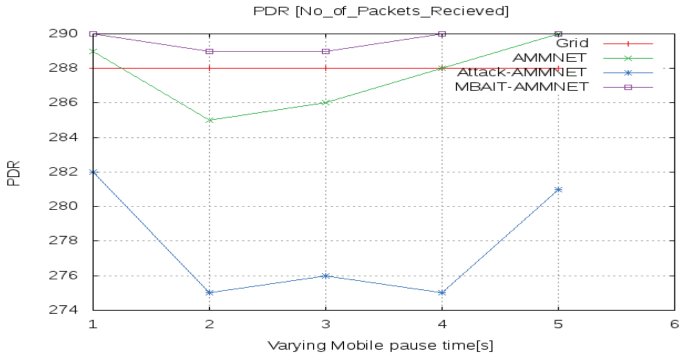


Fig. 9. PDR vs. pause time with constant no of nodes and speed.

2. Throughput:

Pause time will have a significant impact on throughput of the network. Fig 10 shows the impact of pause time on different networks so far compared. Nature of graph shows that as an increase in pause time gives good throughput in the network because of stability of topology. Mbait AMMNET shows an increase in throughput as compared to AMMNET and grid. Under blackhole attack, there is a drastic change in network throughput. Pause time help to stable the network topology that cause to increase in throughput.

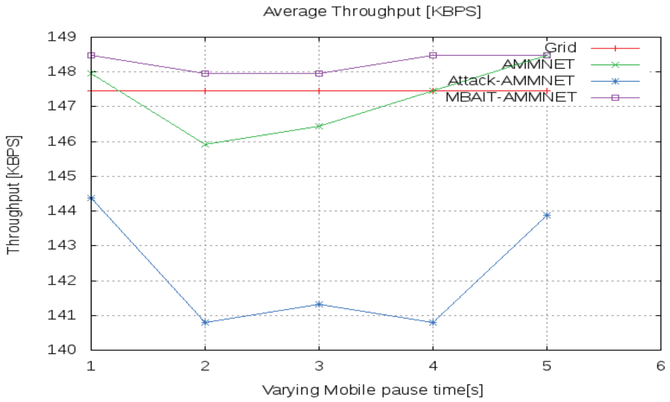


Fig. 10. Throughput vs. pause time with constant no of nodes and speed.

One of the factors maintaining reliability is the security of the network and proposed work will maintain the reliability of the network communication by preventing the malicious attack. This scheme can apply to grid topology that is used by the wireless sensor network.

VIII. Conclusion

With the help of above graphs, it shows that Mbait scheme will efficient to detect and prevent the blackhole attack on AMMNET under AODV protocol. Proposed algorithm will provide security to AMMNET topology and prevent blackhole from the active route. Proposed work will be light weight and achieve good throughput, packet delivery ratio with less delay of packets. Even though the presence of blackhole nodes reliability of the network remained as a normal network. From above results, we conclude that the proposed scheme will efficiently detect and prevent blackhole attack under autonomous mobile mesh network.

References

[1] Wei-Liang Shen, Chung-Shiuan Chen, Kate Ching-Ju Lin, “Autonomous Mobile Mesh Networks,” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, Feb 2014.

[2] B. Salem and J. Hubaux, “Securing Wireless Mesh Networks,” IEEE Wireless Comm., vol. 13, no. 2, pp. 50-55, Apr. 2006.

[3] Ashok M.Kanthe, Dina Simunic and Marijan Djurek, “Denial of Service (DoS) Attacks in Green Mobile Adhoc Networks,” IEEE MIPRO 2012, May 21-25,2012, Opatija, Croatia.

[4] Jaydip Sen, Sripad Koilakonda and Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks," Second International Conference on Intelligent Systems, Modelling and Simulation, 2011.

[5] C. Perkins, E. B. Royer and S. Das, “Ad hoc On Demand Distance Vector (AODV) Routing, Internet Draft,” RFC 3561, IETF Network Working Group, July 2003.

[6] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal, “Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANET,” International Conference on System Engineering and Technology, September 11-12, 2012.

[7] Vani A. Hiremani, Manisha Madhukar Jadhao, “Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET,” International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), IEEE, 2013.

[8] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach,” IEEE system journal, 2014.

[9] D. Johnson, Y. Hu, D. Maltz, “The Dynamic Source Routing Protocol (DSR),” RFC 4728, Network Working Group, February 2007.

[10] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, “SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks,” IEEE Transcations on dependable and secure computing, vol 8, no. 2, March-April 2011.

[11] Sukla Banerjee, “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks,” Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[12] Yanchao Zhang, Yuguang Fang, “ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks,” IEEE journel on selected areas in communications, 2006.

[13] Stuart Russell and Peter Norvig,“Artificial Intelligence: A Modern Approach," Third Edition, Pearson, 2003.

[14] www.nsnam.org