International Journal For Technological Research In Engineering
Volume 3, Issue 10, June-2016 *ISSN (Online): 2347 - 4718*

REDUCING FALSE POSITIVE RATE IN PRESENCE OF BLACK HOLE AND GRAY HOLE ATTACK USING ANAMOLY BASED IDS

Lalita Nayak[1], Vimal Kumar Parganiha[2]
[1]M.Tech, CSE, [2]Asst. Prof., CSE
Disha Institute of Technology and Management, Raipur (C.G.), India

Abstract: Mobile ad hoc networks as we know are the latest trend in the wireless communication technology. It is because MANET has numerous advantages which make it most suitable for applications like natural disaster affected areas, military operations, wild life study etc. As it is becoming popular and being use widely the security risk is also growing. We certainly cannot afford to compromise the security of a network life of many people is on the line for example in case of military operations or scenario of any natural disaster area. There are some loopholes present in the structure of MANET implementation which if not taken care of properly, can result in vulnerable network. Packet dropping attacks are very popular among the other attacks in mobile ad hoc network. In this paper we are presenting a new approach to detect such attacks, which not only detects the malicious nodes in the network, but also has very less percentage of false positive alarms. The reduced number of false positive alarms helps to prevent innocent nodes from being called as guilty and treated as malicious in the network, which in turn increases the network performance.
Keywords: Black Hole, Gray hole, False Positive Rate, IDS, Energy.

I. INTRODUCTION

In our previous work [3] we have discussed about various challenges faced by mobile ad hoc networks. These are mainly because of mobile nature, open communication channel and low resources. All these various challenges leads to making the manet more vulnerable as compared to infrastructure based networks. We will see them here is very brief.

Open Communication channel: It is inherited by wireless network, so this drawback will always be there in MANET. The open channel makes the communication vulnerable, any malicious node can come close to network overhear the traffic. Also packet sniffing and modification are the most common attacks.

Limitation of computing power: Since the nodes do not have high capacity processors they cannot do heavy calculations, it makes securing the network tough[9]. Most of good security mechanisms are based on mathematical expressions, and to make a wireless network secure using those algorithms we have to have good processing capacity in every node, which is not possible in case of mobile nodes.

Limited storage capacity: Mobile nodes are small in size and to keep in that way we have to keep the hardware small, this causes the memory to be kept very small. In large size networks, a single node cannot have all information about the whole network because of lack of memory capacity. This again makes it vulnerable to be attacked[6].

Limited Bandwidth: Wireless channels are not of very high capacity, though we have very high speed bandwidth available in wireless communication. But they cannot be used in MANET as they need additional hardware[8].

II. ATTACKS ON MANET

As we have seen in [3] there are some attacks very specifically designed for mobile ad hoc networks only, most common ones are packet dropping attacks and packet modifications. Major reason behind these attacks being successful is that the routing protocols used in MANET are not designed for being secure. There have been modifications proposed to make it more secure, like MAODV and secure AODV etc. Some of the most common attacks in MANET are discussed here, it will give us idea of various security loopholes present in the mobile network and how they have been exploited by attackers. These attacks can be classified according to their target layers as shown in below table:

Table I. Attacks in MANET

Layer	Attacks
Application Layer	Data corruption, Repudiation.
Transport Layer	Session High jacking, SYN Flooding
Network Layer	Wormhole, Black hole, Flooding, Monitoring, Byzantine, location disclosure etc.
Data Link Layer	Traffic analysis, WEP
Physical Layer	Jamming, Eavesdropping.

We will discuss one attack from each layer here to get idea about the vulnerabilities present in that particular layer.

Jamming: This attack can be seen as DoS attack, it basically targets the communication channel of the network, disturbing the frequencies to make a node unable to communicate with its paired node is the aim of such attacks[7].Attackers use special hardware devices which generate signals to disturb the network communication frequency. Eavesdropping is another attack in this layer where attackers try to trace the data being transmitted.

Traffic analysis: This attack is on Data Link Layer, in this kind of attack the attacker monitors the network for long

duration and they try to analyze the traffic behavior. Depending upon the network activity they decide the target and plan their next attacks.

Black hole attack: In network most of the attacks are performed by malicious nodes including themselves in the network. The malicious node first includes itself in the network and for some time duration it acts as a normal node. But later it starts behaving abnormally, in Black hole attack the nodes includes itself in the communication path, by providing false information (false seq_no). Once the communication starts, it drops all the incoming data packets, making sender-receiver communication fail.

Session High Jacking: Such attacks are more sophisticated, they acquire one complete communication session and performs malicious activities like packet duplication of modification in data etc.

Data Corruption: Data corruption is higher layer attacks where attacker tries to make the data unreadable and useless for the destination node. This is done either by adding some garbage data in the transmitting packet or by altering the bits in the packet in such a way that checksums are not affected. To prevent from such attack packet integrity must hold[5].

III. IDS FOR MANET

To prevent the network from various attacks researchers have proposed numerous intrusion detection techniques. These IDSs are broadly classified into two types Signature based and Anomaly based. The signature based IDSs have a database of malicious behaviors, if a node acts in similar fashion the that node is detected as malicious. Whereas in the anomaly based IDSs the system monitors the network, and traces it's normal behavior. It then keeps record of those activities which are allowed by a normal node, if any node is deviating from it's proper of regular behavior it is considered as malicious.[4]

Existing System: A comparative study of presently available IDSs was shown in(Cite) where we have considered both types of IDSs discussed above. Here we are targeting the detection of Black hole nodes present in the network. In the existing system the detection mechanism for Black hole nodes or any packet dropping node of that matter is basically done by observing the node for dropping of packets. Some IDS uses agents which monitor the nodes and reports about the packet drops, other detection mechanisms monitor the whole network and if there is abnormal packet drops then they declare the dropping node as malicious. These mechanisms which consider only number of packets dropped can result in high rate of false positive alarms. So to reduce the number of false alarms we are proposing a new approach i which we are adding additional layer of verification about a node being malicious. We will discuss the idea in the next section in detail.

IV. PROPOSED IDEA

As we discussed in above section there are various IDS present to detect malicious nodes in a mobile ad hoc network. Also we studied that not all of them are performing in the same manner for different kind of networks; some IDS may work better than others in low mobile network, where as other can perform better if there are dense nodes in the network. The algorithms we studied so far in the literature survey, they mostly focus on either to reduce the communication overhead [1][2] or to decrease the computation overheads on few selected nodes. IDSs have different types and they are used to detect malicious nodes in the network. The IDSs we saw in the previous section were majorly detecting packet dropping nodes and working good against such attacks like Black hole and Grey hole attacks. Mostly to detect such packet dropping attacks existing systems uses packet dropping as a detection criteria. Meaning that if a particular node is dropping most of the packets it receives then they are declared as malicious node and an alarm is raised by the IDS. In this paper we are presenting a new detection method to narrow down the false-positive rate of IDS.

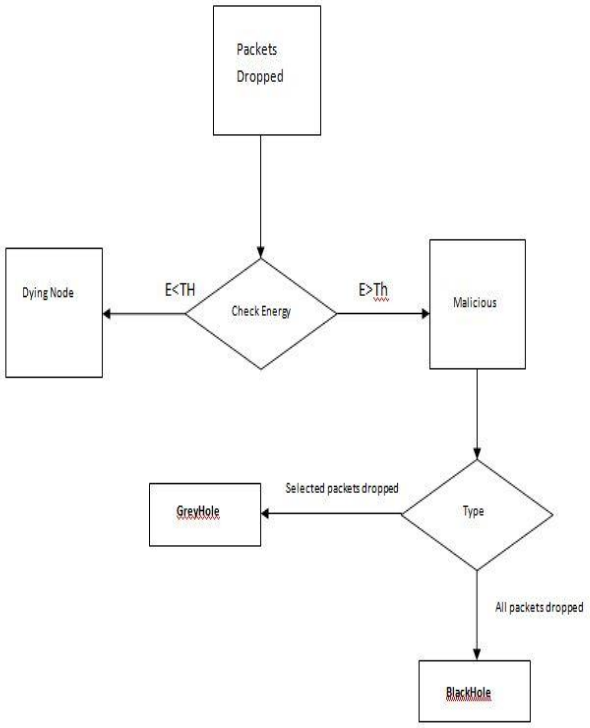

Fig. 1 Design flow of proposed Idea

In existing IDSs once a packet is caught for dropping a lot of packets, they are declared as malicious without any further investigation. There may be situation that the victim node is not malicious and reason for dropping the packets are genuine; one of the most common reason can be energy level. If a node is not having enough energy to forward the packet to the next node then it will simply drop the incoming packets. In routing algorithms like plain AODV the nodes take participate in communication channel using hello packets, and the sender node start sending packets through that node without taking note of any other parameter. In this proposed method we are presenting another layer of detection based on energy of a particular before declaring it as a malicious node (as shown in the above figure). When a node is detected for dropping huge number of packets, the

IDS will not raise the alarm directly, Instead we will check energy level of that particular packet dropping node. If the energy is below the threshold limit then it will not be declared as malicious but if the node is having enough energy to forward the packet and still it is dropping them it will be classified as malicious node and an alarm will be raised. Advantages: The proposed method will reduce number of false-positives. If a node is not malicious and any IDS system is detecting it as malicious then we call it a false positive case. In the proposed system the nodes which are dropping packets because they do not have sufficient energy will not be called as malicious so it will not generate false alarm as other IDSs do.

V. IMPLEMENTATION

In the implementation we have taken NS2 simulator to create the test environment. Some of the parameters are pre-defined for smooth simulation (like: packet size, channel bandwidth, traffic type etc). We created a normal network with some normal (non-malicious) nodes, and used plain AODV protocol for routing. Later we put some fig.malicious nodes which are performing packet dropping attacks (Black hole and Gray hole attacks). The IDS is detecting the malicious nodes on the basis of number of packets dropped; if it finds any node dropping more packets it checks the energy level of that particular node. If the node is having sufficient energy and still it is dropping the packet then it is declared as malicious; but if the is running out of energy then it will not raise the alarm. To implement and detect attacks we have made some changes in the aodv.cc and other support files. The simulation was run for multiple times with same configuration. The configurations were changed to get more clear results based on different network size and with changing number of malicious nodes present in the network.

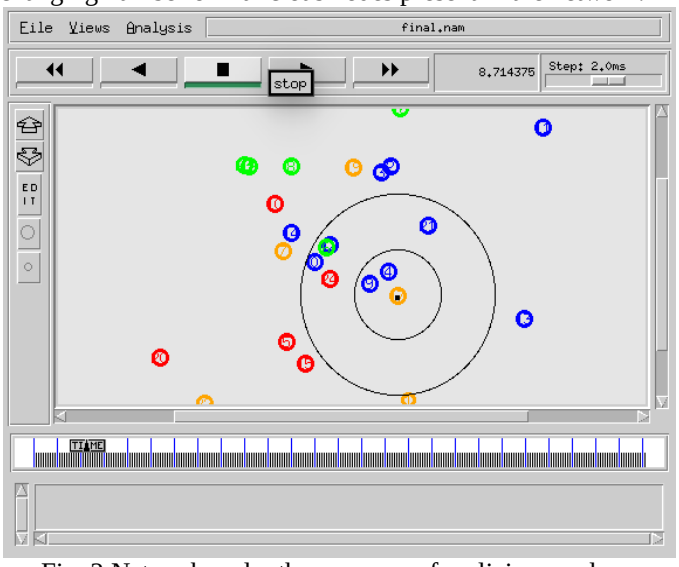

Fig. 2 Network under the presence of malicious nodes

We have done simulation by network simulator 2(NS2). In following scenario malicious node detracting source and not forwarding the packets to destination which is showed in fig. 2. IDS will check energy level of that victim node is it above the threshold value or not. If the energy level is low and packet is dropped it is not an attack. If energy is high and still packets are dropped and then checked the node. This function is showed by Fig. 3

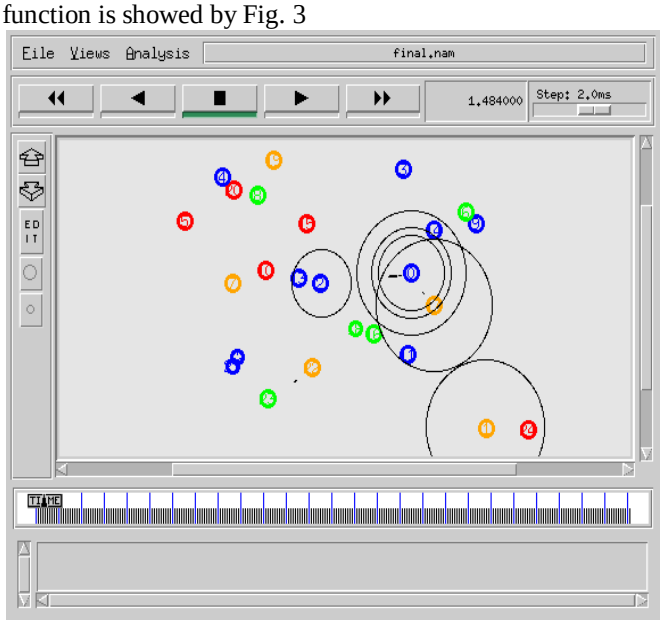

Fig.3 IDS check victim node

VI. RESULTS

We simulated the above proposed idea on NS2 as discussed in the previous section. To get near accurate results we have run the simulation 10 times for each configuration, and taken the average value as final. The results are shown in tabular form as below:

Table II Result Analysis

Sr No	No of total nodes	No of actual malicious	No of malicious nodes detected	False positive alarms	% false - positive
1	10	2	2	0	0
2	20	4	4	0	0
3	30	6	6	0	0
4	40	8	9	1	2.5
5	50	10	12	2	4
6	60	12	13	1	1.6
7	70	14	16	2	2.85
8	80	16	16	0	0
9	90	18	19	1	1.1
10	100	20	20	0	0

Average % false positives: 1.20

VII. ANALYSIS

The above results shows that the proposed system is detecting malicious nodes successfully and the same time it is giving very low percentage of false positive alarms. In this way it improves the network performance and also reduces the number of non-guilty victim nodes, which can be used as a part of network once they have their power source replaced.

REFERENCES

[1] G. Eason, B. Noble, and I.N. Sneddon, "Improving AODV protocol against blackhole attacks." international multiconference of engineers and computer scientists. Vol. 2. 2010.

[2] KaewTraKulPong, Pakorn, and Richard Bowden. "An improved adaptive background mixture model for real-time tracking with shadow detection."Video-based surveillance systems. Springer US, 2002. 135-144.

[3] Lalita Nayak, Roopal Lakhwani, "MANET Security Issues and Solutions : A Review", International Joural of Science and research Technology, Vol.2 Issue 4, April 2016, 2395-1052

[4] L. Qian, N. Song, and X. Li, "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path", Wireless Communications and Networking Conference, 4:2106 -2111, Mar. 2005.

[5] S. Capkun, L. Buttyan, and J. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks", Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, pages 21-32, 2003.

[6] Mohit Jain,Himanshu Kandwal, "A survey on complex wormhole attack in wireless Ad hoc Networks" ,International conference on Advances in Computing, Control and telecommunication Technologies,2009,IEEE,555-558.

[7] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proc of First IEEE International Workshop on Sensor Network Protocols and Application (SNPA03), pp. 113-127, May2003.

[8] Rutvij H. Jhaveri "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs" Third International Conference on Advanced Computing & Communication Technologies 2012.

[9] Kurosawa, S., Nakayama, H., Kat, N., Jamalipour, A., and Nemoto, Y. Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method. International Journal of Network Security, 5(3):338–346, November 2007.

