Mitigating Black Hole and Gray Hole Attacks in MANETs using ID3

Shilpa
Department of Electronics and Communication Engineering
Shoolini University of Biotechnology and Management Sciences, Solan, Himachal Pradesh, India

Vivek Kanwar
Department of Electronics and Communication Engineering
Shoolini University of Biotechnology and Management Sciences, Solan, Himachal Pradesh, India

Abstract- Security is the vital part of any communication link. However MANETs have self-configuring and self-maintenance capabilities, but secure communication over MANETs becomes one of the most challenging task. Due to mobile nodes and the dynamic infrastructure of the network the security protocol designed for other networks do not work well in MANETs. Also many techniques have been developed to identify different types of network attacks, the black hole and gray hole attacks are two major attacks on MANETs. In this paper, we presented a technique to mitigate the gray hole or black hole attacks in the mobile ad hoc network, using AODV (Ad hoc on demand routing protocol). Moreover, ID3 algorithm is used to diminish black hole and gray hole attacks.

Keywords – Routing, Black hole, Gray hole

I. INTRODUCTION

MANET is a multi hop wireless network, formed dynamically from a collection of mobile nodes without the any centralized coordinator. The nodes communicate to each other by means of one or more intermediate nodes, that is, every node in MANETs act as a router. In recent years, MANETs have received tremendous attention because of their self-configuration and self-maintenance capabilities [1], also they can communicate with a wired network using gateways. MANETs are very flexible networks, they can easily accommodate additional nodes to them. But due to this nature of MANETs and due to their dynamic topologies, mobile nodes, and packet forwarding technique used for communication, secure communication over MANETs becomes a challenging issue. Black hole attacks and gray hole attacks are the most common attacks in MANETs. These attacks are carried by the malicious nodes present in the network, which are difficult to detect in this type of dynamic, infrastructure less network.

The rest of the paper is organizes as follows. Previous work done in the field of security of MANETs is explained in section II. Proposed work to eliminate gray hole and black hole attacks are explained in section III. Results and conclusion of the work are presented in section IV.

II. PREVIOUS WORK

A. Proactive and reactive approach –

The various approaches for the security in MANETs are categorized in two type: proactive approach attempts to prevent security threats in the first place, typically through various cryptographic methods. The reactive approach on the other hand performs the detection and recovery procedure [2]. The most secure routing protocols adopt the proactive approach in order to secure routing messages exchanged between mobile nodes, while protect packet forwarding operations are generally protected using reactive approach. The prevention component in MANETS is mainly achieved by using some secure ad hoc routing protocol such as DSR, AODV routing protocol that prevent the attacker from installing false routing states at other nodes.

B. AODV based MANETs–

Black hole and gray hole attacks are the most important security problems in MANET. Black hole starts in route discovery phase and gray hole as an attack which drops packets in transmitting step [3]. Detection of gray hole is more difficult than black hole, because the attacker works as normal node then starts dropping of data. some of the proposed works are introduced to detect black and gray hole attacks, pointed out their advantages and disadvantages and at the end, these methods are compared from some aspects.

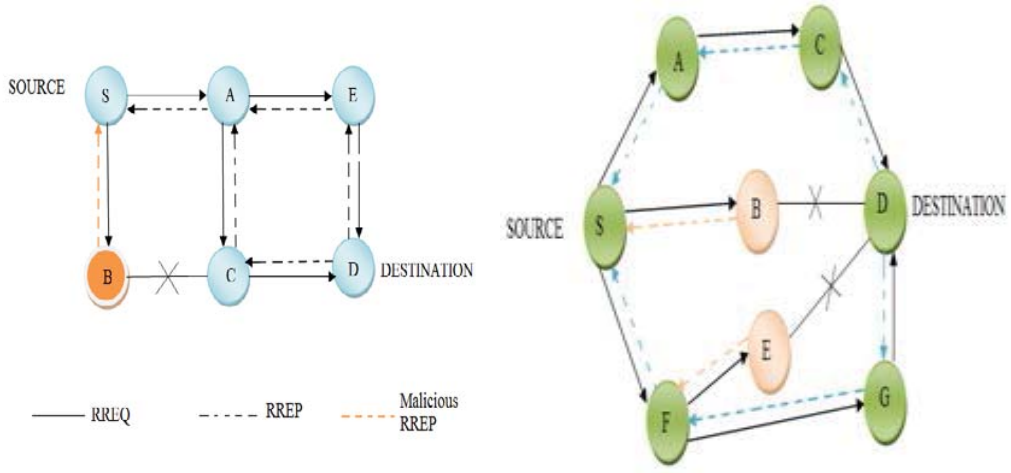


Figure 1. (a) Black Hole Attack (b) Gray Hole attack

C. MANETS in Group Formation–

Nodes are considered in multiple groups using the same interface and a hierarchical traffic pattern usual of a tactical operation [4]. It is shown that the inter-group SAs, between group heads, requires a different trust model than that of intra-group SAs in order to keep overhead of authentication manageable. The results also show that for group heads, the number of hops is a more effective parameter to which their SA duration should be adapted than their actual link distance modeled by FER.

D. Route Discovery in MANETs–

From both efficiency and security point of view, the route discovery in MANETs is a vital task. A model was represented by Acs, Buttya´n, and Vajda in this direction. Among the novel features of this security model is that it ensures the security guarantee under concurrent executions, an feature of crucial practical implication for this type of distributed computation. A novel route discovery algorithm called endairA was also proposed, together with a claimed security proof within the same model. In this paper [5], it is showed that the security proof for the route discovery algorithm endairA is false, and moreover, this algorithm is vulnerable to a hidden channel attack. Also, the security framework that was used for route discovery, and argue that composability is an essential feature for ubiquitous applications is also analyzed.

E. Enhanced Adaptive Acknowledgment (EAACK) for intrusion detection–

In this paper, a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs is proposed and implemented [6]. Compared to contemporary approaches, EAACK demonstrates higher malicious- behavior- detection rates in certain circumstances while does not greatly affect the network performances. Reduce the network overhead caused by digital signature examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre distributed keys, testing the performance of EAACK in real network environment instead of software simulation.

F. Adaptive Secured Multipath for Ad hoc networks (ASMA) –

Adaptive Secured Multipath for Ad hoc networks (ASMA) is a scalable, flexible and application-oriented to manage security depending on the application requirements and the network security conditions [7]. ASMA is based on framework able a structure called macrograph combining both dynamic trust management and multipath routing. The macrograph structure is capable to estimate transmission security in order to assure that communications are established only when they match applications security requirements. ASMA flexibility offers compliance with most on demand routing protocols and security tools.

G. Security Evaluation Model–

A dynamic security evaluation model is given by Mu Haibing to measure the security of distributed trust third party (TIP) applications based on threshold cryptography in mobile ad hoc networks (MANET) [8]. Firstly, the attack process and build an attack model are studied using stochastic process approach. A dynamic evaluation model is proposed in the following which can give the proper value of threshold and updating period of sharing secret.

H. Decision tree construction using ID3–

Bhardwaj and Vatta [9] described the implementation of the ID3 algorithm and created a decision tree. In inductive learning Decision tree algorithms are very famous. For the appropriate classification of the objects with the given attributes inductive methods use these algorithms basically.

These algorithms are very important in the classification of the objects. That is why many of these algorithms are used in the intelligent systems as well. In this paper the ID3 decision tree learning algorithm is implemented with the help of an example which includes the training set of two weeks. The basic calculations are used to calculate the classification related to the training set used.

III. PROPOSED ALGORITHM

This paper presents an algorithm to mitigate black hole and gray hole effect using ID3 and AODV as routing algorithm.

1. Declare n packets, P1, P2 …., Pn each Packet containing R Acknowledgments A1, A2…..Ar, C number of class or address values C1, C2….Cc.
2. For packet Pi where (i = 1; i<=n; i++)
   {
   If(R is Empty)
   {
   Return a leaf node with class value,

   }

   Else If (All the transaction in T(Pi) have the same class)

   {
   return a leaf node with the class value.
   }

   Else

   {

   Calculate Expected Information classify the given sample for each packet Pi individually.

   }
3. Calculate Entropy for each Acknowledgment A1, A2,…., AR of each packet Pi.
4. Calculate Information Gain for each Ack (A1,A2…., AR) of each packet Pi.
5. Calculate Total Information Gain for each Ack of all packets
6. A Best Acknowledgment will be the one having Maximum Information Gain.
7. Let V1, V2…., Vm be the value of ACK.
8. A Best Ack partitioned P1, P2,…., Pn packets into m packets.
   P1(V1),P1(V2),.....P1(Vm),.....P2(V1),P2(V2).....(Vm),.....Pn(V1),Pn(V2),.....Pn(Vm).
9. Return the Tree whose Root is labeled as ABestAck and has m edges V1,V2.....Vm.
10. Such that for every i the edge Vi goes to the Tree.
    ID3(R – ABestAck, C, (P1(Vi), P2(Vi)……. Pn(Vi)))

A. Flow of Work

At first the scenario is selected under which we want to apply our algorithm. We have made a simulation of 100 nodes which are plotted in the MATLAB environment. The all process run 5 times. We can make a suitable path with the help of AODV algorithm. AODV is applied every time to find the secure path or to prevent from black hole attack and gray hole attack. Now, decision tree is created by the help of ID3.

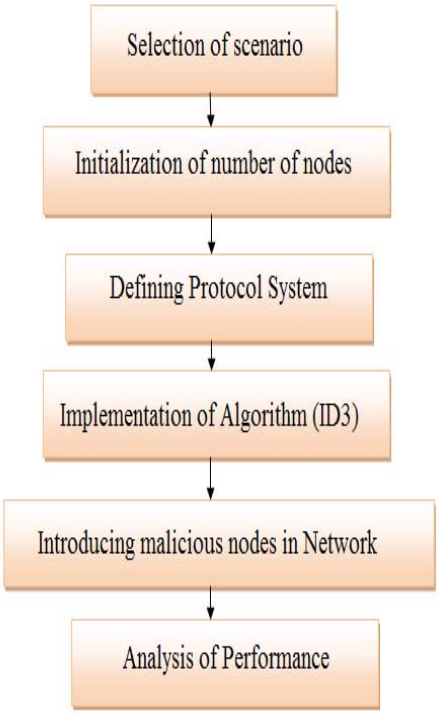


Figure 2. Flow of Work

IV. RESULTS AND CONCLUSION

The results shows that the proposed technique is a promising solution to avoid black hole and gray hole attacks. Our system shows up to 13 kbps throughput and a very low delay with cache in MANETs. Packet delivery is achieved up to 98%. Future efforts can be made to further improve the algorithm to prevent all types of attacks on MANETs. The given figures show the parameters on the basis of which performance of this paper is calculated. First found the nodes in the network which are shown in the figure given below:

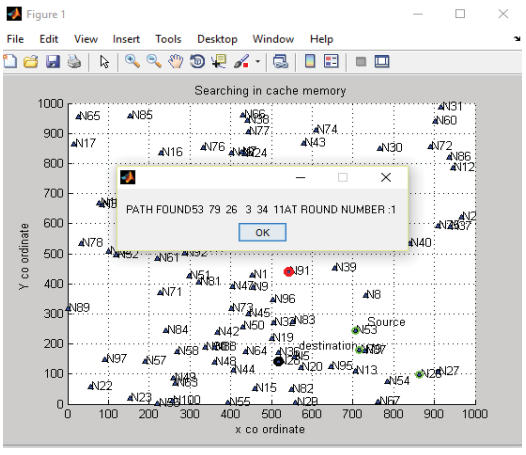


Figure 3. Path Found in First Round

Like the figure given above all five rounds are calculated in the cache and with the help of the ID3 a decision tree is formed by calculating entropy at each node which should be followed first. This is totally dependent on information gain which shows a more secure network.

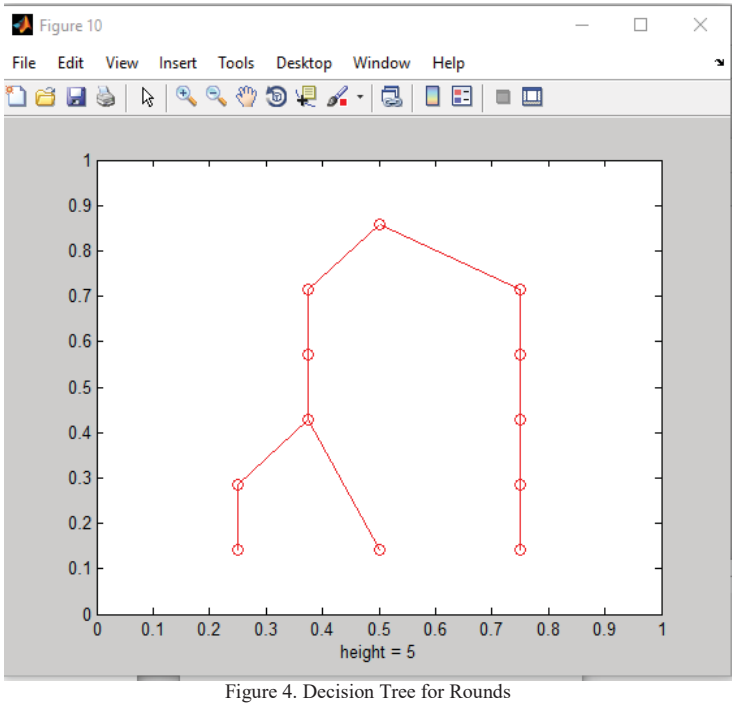


Figure 4. Decision Tree for Rounds

After drawing the decision tree, it is clearly shown that the root node is secure from black hole attack. After detecting the black hole attack our performance can be explained in terms of node to node delay, packet delivery ration etc.

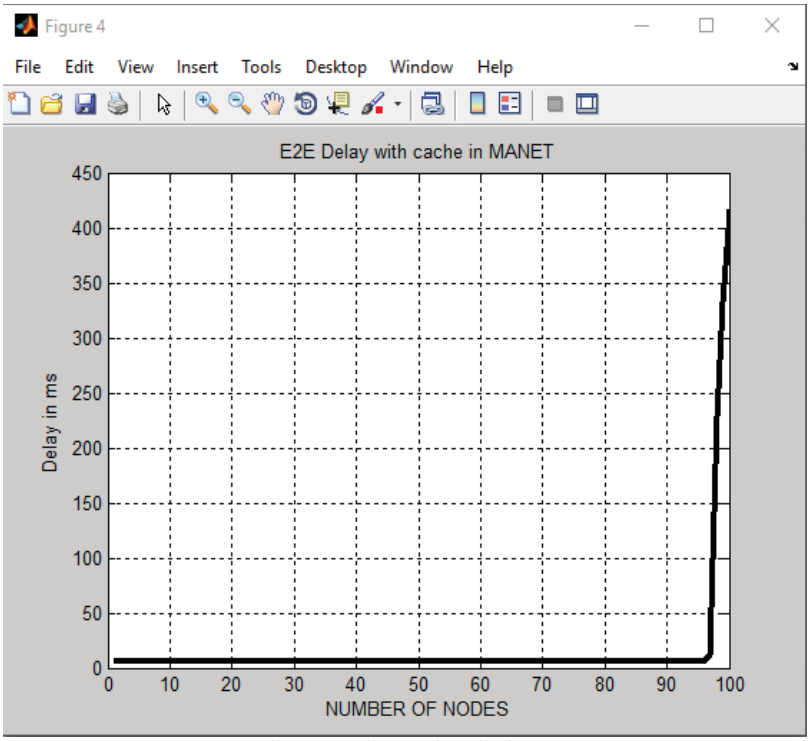


Figure 5. Node to Node Delay in ms

This shows that when the number of nodes crosses 97 delay increases sharply and at 100 it becomes approximate 400 mili second.

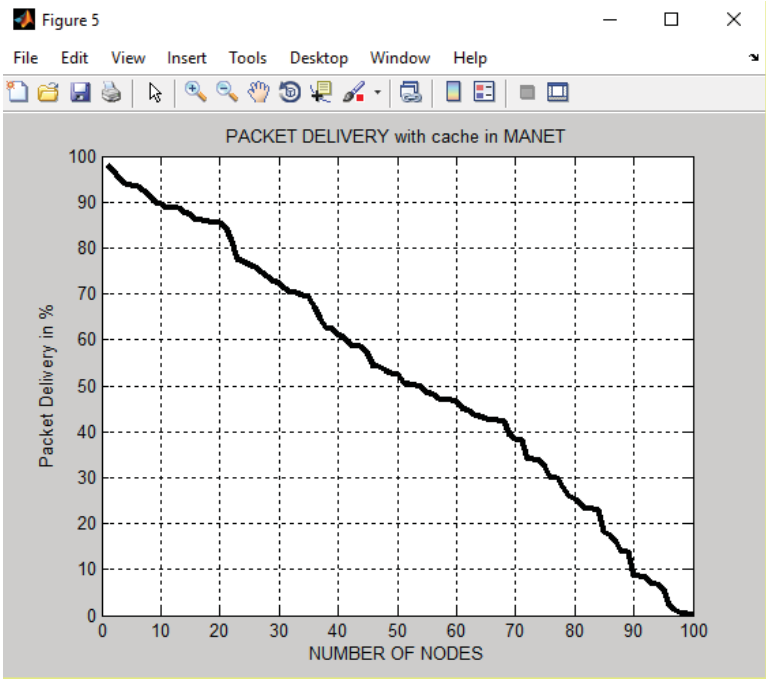
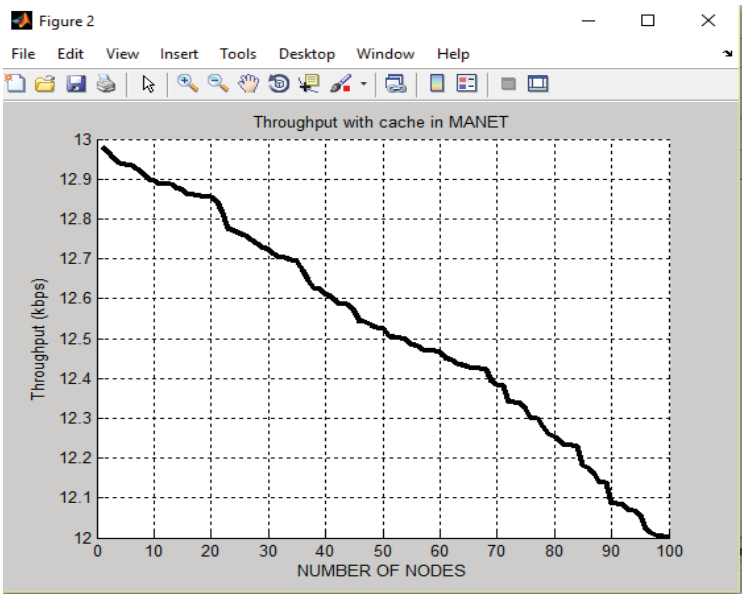


Figure 6. Packet Delivery

We can see easily from the given graph when number of nodes are 10 then packet delivery ratio is 90 percent as we go on increasing it starts decreasing and at 100 nodes it becomes almost zero.



Figures 7. Throughput of the MANET

This figure shows that as the nodes increases the throughput decreases.

REFERENCES

[1] Richard For, Michael Howard, "Security in Mobile Ad Hoc Networks", IEEE Security and Privacy, 2008.
[2] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang**, "**Security in Mobile Ad Hoc Networks: Challenges And Solutions**",** IEEE Wireless Communications, February 2004.
[3] M.K. Rafsanjani, Z.Z Anvari and S. Ghasemi, "Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET", IJCA Special Issue on Network Security and Cryptography, pp. 11-17, 2011.
[4] Mazda Salmanian, Li Pan, Jiangxin Hu, Ming Li, "On the Efficiency of Establishing and Maintaining Security Association in Tactical MANETs in Group Formation", The Military Communication Conference, 2011.
[5] Mike Burmester, Breno de Medeiros, "On the Security of Route Discovery in MANETs", IEEE Transactions on Mobile Computing, Volume 8, No. 9, September 2009.
[6] E.M. Shakshuki, N. Kang and T.R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transaction on Industrial Electronics, Volume 60, Issue 3, pp. 1089-1098, 2013.
[7] Vincent Toubiana, Houda Labiod, "Towards a Flexible Security Management Solution for Dynamic MANETs", IEEE, 2008.
[8] Mu Haibing, Zhang Changlun, "Security Evaluation Model for Threshold Cryptography Applications in MANET", Volume 4, IEEE, 2010.
[9] A. kumar, H.C. Maurya and R. Misra, "A Research Paper on Hybrid Intrusion Detection System", International Journal of Engineering and Advanced Technology, Volume 2, Issue 4, pp. 294-297, 2013.