ISSN:2231-0711

Devideen Ahirwar et al | IJCSET(www.ijcset.net) | 2018 | Volume 8 Issue 4, 52-55

Comparative Study of Black Hole Attack Detection in MANET using various IDS Methods and DRI Table

Devideen Ahirwar and Shailendra Satyarthi
Department of Information Technology
Dr. B. R. Ambedkar Polytechnic College, Gwalior, MP, India

Abstract: Mobile Ad hoc Network (MANET) is one of the Ad-hoc networks with mobile nodes. Dynamic topology, no permanent infrastructure, no central administration are feature which makes. AODV routing protocol is insecure from various attacks. Black hole attack is one of them, where malicious nodes provide the false routing information to network and attract all data packets toward themselves showing the shortest path. In this research paper, we compared Black Hole attack detection and prevention methods using IDS techniques and DRI table. The various IDS techniques described are Artificial Neural Network (ANN), Fuzzy Logic, Genetic Algorithm, Prime Product Number (PPN) and Machine Learning. In comparison IDS techniques may be better techniques in future as compared with DRI table, as drastic increase of computational power and memory of computer system.

Keywords: MANETs, AODV protocol, Black hole attack and malicious node, IDS, DRI Tables.

INTRODUCTION

In following type of Network a collection of mobile nodes that organize a network device without outer predefine infrastructure or central based operation management [7]. Also this network is an IP based n/w collected by a no. of wireless and Mobile Nodes linked with microwave & radio systems [13]. Following network provide unique and attractive feature with No fixed infrastructure, centralized administration, self configuration with automatic, self maintenance and quickly deployment. MANETs communication provide with each node free to join, move and leave indirectly and independently [16].

This research paper propose with secure route discovery and maintenance methodology based on evaluate Black hole attack based technique with performance analysis and detectable malicious node technique and also analysis prevented mobile nodes technique. Following performance evaluation techniques evaluate important Ad-hoc on demand distance vector (AODV) routing protocol also is standard MANETs protocol [12], [15]. MANET is a mostly effected black hole attack. Attacker used with and without attack mobile nodes with provided malicious nodes, shortest route and high destination sequence number [13].

Our research papers provide performance evaluation for later research work on MANET used intrusion detection system based technique with comparative Data Routing Information (DRI) table's method [15].

AODV

It is a reactive protocol and standard types of protocol used by an Ad-hoc network [9]. Also capable of these protocol Broadcast, Unicast and Multicast routing. In this protocol provide by route maintenance and discovery with generate following three types of packet message i.e. RREQ, RREP and RERR [11].

Mostly attacker is generating malicious node with RREP message and misbehavior information generate some of related source node. It is possibility for the attacker to include forged information in the RREP message [10].

Every AODV routing protocol contains following route table entry information:

- Destination node
- Next hop
- No. of hops
- Destination sequence number
- Active neighbors for the route
- Expiration timer for the route table entry

Black Holes Attack

It is a kind of DOS types attack in MANET. These attack main parts of network layer. In this attack, Attacker provided malicious node uses this reactive type protocol to advertise in shortest route and high destination number [13]. Also this attack easily implement with AODV protocol during the route discovery process. And the outcome of this type of attack can be varying. Black holes attack is a classified into two categories i.e. single and cooperative attack [12], [15].

In this attack provide following activity over network scenario [10].

- Malicious node detects the active route and notes the destination address.
- Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
- Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
- The RREP received by the nearest available node to the malicious node will relayed via established inverse route to the data of source node.
- The new information received in the route reply will allow the source node to update routing table.
- New route selected by source node for selecting data.
- The malicious node will drop now all the data to which it belong in the route.

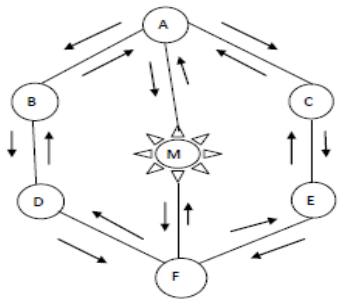

Fig.1: Black holes attack

As in fig.1 M is the malicious node which gives false data routing information to the node, which is requesting shortest path to the destination node by using RREQ, that is having shortest route to the destination using RREQ and all the data packets send by the source node.

Here let Node A desire to send data packets to Node E so A Node request to shortest route by sending RREQ to its corresponding Nodes and every corresponding node replies (RREP) with number of Nodes to destination Node. But black hole/ malicious Node M replies false number of Node to Destination Node or having shortest path. Then Source Node sends all packets to M and all packets drop, which is black holes attack. In cooperative attack, there is more than one malicious Node in the Networks.

Intrusion Detection System (IDS)

IDS are widely used tool for detection and of removal of intruder attack in the unauthorized access to MANET.

IDS node's actions for RREQ, RREP packets:-

RREQ: First IDS checks if there is an entry in its table for destination & source .IDS adds source, destination and all nodes which are going to broadcast nodes in table. These broadcasting nodes ID are used for detection of attack [17].

RREP: It stops to checking if the source is destination. If answer is no then it check if there is an entry for this node in its table as broadcasting node or not. If it is not last broadcast node then it starts a counter and named that node as inactive. If it cross the maliciousness over a predefined value, marks that node as active and sends messages to n/wk that called block and announces that is malicious node [17], [16]. It is provide following important advantages:

1. It uses new nodes which called IDS.
2. It gives more trustful reporting of black hole attacks.
3. It is used for decreasing the overhead for monitoring on all nodes.
4. There are less chances of mistake in detecting the malicious node.

IDS are too classified in two categories depending on detection methods.

1. Intrusion behavior is identified by using observed data as misused detection; here low false positive rate can be used to detect prominent intrusions. Misuse technique fails to detect unknown intrusion. To overcome the frequent involvements of intrusions problem, the only way is learn from all intrusion and update the knowledge very frequently. This task can be done automatically by using the super wised learning technique. As the training data preparation (Classify as data normal or intrusion) is difficult and expensive to get rid on this approach the anomaly detection is better one. Learn from previous experience.
2. In Anomaly detection technique, undesired activity is performing. Anomaly can be detected by using the deviation in observe data from normal. Anomaly detection techniques are of two types. Static anomaly detection technique which assume no change in behavior of investigation target. Another type anomaly is dynamic anomaly detection technique where behavioral habits of and users/ networks/hosts are extracted as pattern.

In this intrusion detection systems used following broad techniques in detect and prevent Black hole attacks. Also minimize routing overhead, energy consumption and throughput. These current research paper describe technique with optimize previous research and provide current usable research on black hole attack.

1. Artificial Neural Networks based Research: ANN is an idea to simulate the functioning of Biological Nervous System on computer. ANN has the capability of learning by using supervised or unsupervised learning. Learning ability is high computation, Prediction of unknown Pattern and some advantages of ANN.

Exiting research work [8],[4] considered feed forward and back propagation ANN model with used four input i.e. Packet loss, Packet sending, packet receiving and Energy Consumptions, Two hidden layer and one output layer, to design a mechanism for Intrusion detection under DOS attacks in MANET. Also these input parameters used as to train and learn the system. And this paper optimum model based hints provide if used Levenberg-Morquardt (LM). LM algorithm used the training set capability is large, if networks size is moderate with memory reduction feature. So that LM training algorithm is work fast.

But our proposed research provides if intruder and malicious node injects a big data amount of junk packets into the network and causes dos of the attacked. So that LM training algorithm is done by using big data based model work because data size medium and low is not suitable. If input parameter when used directly without security i.e. cryptographic algorithm. Black hole attack is a vulnerable and more complicated attack so that these systems not suitable used directly input based parameter. Also result better if ANN based system used with fuzzy logic things. And proper input parameter selection is important factor for getting better results in black hole attack.

2. Fuzzy Logic Based Research: Fuzzy logic technique is the not old vital technique but used early few years. This technique used in intrusion detection with black hole attack based on uncertainty and complexity with derived human reasoning. Also this technique finds secure routing with AODV protocol in wireless Ad-hoc networks. Fuzzy logic provides the strength to obtain the uncertainties associated with human process. The need of fuzzy logic arises in the time to describe the principle of and problem of uncertainty. It is a rigorous mathematical field, and it

provides an effective vehicle for modeling the uncertainty in human reasoning [1].
The proposed heuristic algorithm based technique with successfully detect black hole attack in MANET with also information passed to other nodes [2]. This technique weak point if the performance of network falls to a very minimum low value under the black hole attack.
But our proposed research scheme not only detect the malicious node based on black hole attack in stage of data transmission with isolates it from the network. In this scheme also helpful fuzzy variables or linguistic terms and fuzzy interference system (FIS) used on identify degree of malicious node with if-then-else rules are used to define all stages tn the network for identify the black hole attack and intrusions.

3. Genetic Algorithm based Research:

It is a Meta heuristic inspired by the process of natural selection that belongs to the larger class of evolutionary algorithms (EA). Genetic algorithms are commonly used to generate high-quality solutions to optimization and search problems by relying on bio-inspired operators such as mutation, crossover and selection. Also these algorithms provide large research in computer science and operation research.
This algorithm based on stochastic technique with real solid progression with developed Charles Darwin in 1858.
It genuinely is designed ordinarily around the thoughts from the headway by means of sound collection, utilizing a person of people that will continue the decision strategy as far as variety actuating administrators, for example, transformation and in addition recombination (crossover). An activity capacity is used to gage individual, and also regenerative framework accomplishment ranges with wellness [6].
Particle Swarm Optimization is developmental calculation in view of swarms and it has been presented by Kennedy. It is other most useful technique in with genetic algorithm. And PSO offers many elements with other developmental calculations. The framework is instated with number of populaces [6], [5]. At that point hunting down optima is finished. Not at all like GA, has PSO had no administrators like change, wellness and so forth.
In PSO, there are potential arrangements called PSO. So, PSO algorithm can be represented as below;
a) Evaluate the objective function of each particle.
b) Create initial particles.
c) Choose new velocities
d) Update each particle location.
e) Iterate until a solution is reached.
These techniques also provide MANETs based different attacks removed i.e. black hole attack and other.
As genetic algorithm optimize the searching problem using intelligent exploitation method. It is the main technique to simulate the processes for evolution [6]. The main benefit provides AODV routing protocol is minimum setup connection and delay with assignment of destination sequence number to identify latest route. Black hole attack is the network layer attack and network susceptible to various hazards with this attack.
But our research based scheme is provide IDS specification with analyzed with any abnormality detected. These techniques based on genetic algorithm approach with analyzed behaviors of every node and provide detail things about the attack on genetic algorithm controller.

4. Prime Product Number (PPN) based Research: In PPN, the prime number is assigned. To each node for node identity and it is not changed.
PPN scheme based research paper where MANET organized into number of clusters. Each node in member of at least one cluster and have prime number for node identity [3]. Every cluster has cluster head and keeps the neighbor information in table the change into RREP packet message format. Intermediate node provides the information of its cluster head and product of all prime numbers from destination to source node in the form of PPN. By using RREP message to source node. The source node checks the reliability of intermediate node.
Also this proposed scheme provide secure routing at the cost of high overhead and when malicious node is out of the cluster.

5. Machine Learning Technique based Research:

It is a subset of artificial intelligence in the field of computer science that often uses statistical techniques to give computers the ability to "learn" (i.e., progressively improve performance on a specific task) with data, without being explicitly programmed. It is closely related to (and often overlaps with) computational statistics, which also focuses on prediction-making through the use of computers.
In order to classify this data a number of machine learning techniques are available. In order to develop such kind of data model the following algorithms are frequently utilized for learning and identifying the attack pattern [1].
In this learning technique provide two major techniques based on AI and Neural Network i.e. supervised learning and back propagation network.
And existing research work provides this technique data model and linear classifier with represent of space and mapped in prediction. Also simply used each input layer weights without encryption and cryptographic algorithm. So those attackers mostly Black Hole attacks easily include malicious node and defect network with specific packets.
But our proposed scheme based on artificial intelligence with learning latest developing tools. With used following technique heuristic pattern, optimization and cryptographic technique based natural language processing.

Data Routing Information (DRI) Table

In this approach each node of MANET maintains DRI table. This DRI table keeps information about all its neighbors Due to the dynamic change with time in network topology frequent change takes place in DRI table. DRI table is used to check whether RREP message from legitimate node [7], [12].
In this paper DRI Table maintains information of neighbors ID, from and through data packet. Using DRI table identify the trustable node. As RREP received from malicious node

with high sequence number, the next hop node and previous hop node is checked with DRI entry. If match not found, it is notified to other nodes in MANETs about this malicious node and every node make DRI entry to "NULL" for this node.

Advantages:

1. This method detects co-operative black-hole attack.
2. This method reduced packet overhead and processing time for detecting malicious node.

Disadvantages:

1. If there is no any attack in n/w then this process consume lot of time and create overhead.
2. It fails to detect Gray Hole Attack.

CONCLUSION:

This research paper present a survey with review on the various methods of Intrusion Detection System in comparative DRI Tables in black hole attack with standard AODV protocol on MANETs. These papers also focus various tools and technique IDS based method. In future evaluate various parameters i.e. packet delivery ratio, end to end delay, throughput and average jitter with implement network simulator and other tools.

REFERENCES:

1. P.N. Raj and P.B. Swadas,"Dpraodv: A dyanamic learning system against black hole attack in AODV based MANET". Arxiv preprint arXiv: 09092371, 2009.
2. Moh. A. Azim, H.E.D Saleh and M.Ibrahim, "Black Hole Attack detection using Fuzzy based IDS." IJCNIS, vol. 9, No.2 Aug 2017.
3. Sapna Ganbhir & Saurabh Sharma, "PPN Prime Product Number based malicious node detection scheme for MANETs. 3rd IEEE IACC PP9781467345293 Years 2012.
4. R & A Kaur, "Black hole detection in MANETs using ANN." IJTRE, ISSN 23474718 may 2014.
5. Kanika Bawa & Shashi B. Rana, "Prevention of Black hole attack in MANET Using addition of Genetic Algorithm to BFO." IJCET, Aug 2015, ISSN 22774106(E), 23475161(P).
6. K.S. Sujatha, V.Dhrmar, R.S. Bhuvaneswarabn, "Design of genetic algorithm based IDS for MANET." IEEE, ICRTIT 2012.
7. Seryvuth Tan & Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV- based MANETs". IEEE ICTC 2013.
8. Zahra Moradi & M. Teshnehlab, "Implementation of Neural Networks for intrusion detection in MANET." IEEE proceedings of ICETECT 2011.
9. C. Perkins, E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," The Internet Society 2003.
10. M K Parmar and H B Jethva, " Survey on Mobile ADHOC Network and Security Attacks on Network Layer", in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Vol 3, Issue 11, Nov 2013 ISSN: 2277 128X.
11. Devideen Ahirwar & Prof. Sarvesh S. Rai, "Improvement of AODV routing protocol Algorithm with Link Stability and Energy Efficient Routing for MANET. IJCSET, ISSN 22310711 Feb 2014.
12. Saeed K. Saeed & N. A. Noureldien, "A detection and prevention algorithm for single and cooperative Black hole attacks in AODV MANETs." IARIA, 2015, ISBN 9781612084275.
13. P.K. Singh & G. Sharma, "An efficient prevention of Black hole problem in AODV routing protocol in MANET." IEEE 11th ICTSPCC 2012.
14. Ankito Mehto & Prof. Hitesh Gupta, "A Dynamic Hybrid approach for wormhole detection and prevention." IEEE 31661 4th ICCCNT 2013.
15. M.K.Rafsanjani, Z.Z. Anvari & S. Ghasemi,"Methods of preventing and detecting Black/Gray Hole attacks on AODV-based MANET." IJCA issue on NSC 2011.
16. Gurpreet Singh & Dr. Raman Maini, "Comparative analysis of various Black Hole Detection techniques." IJLTEMAS, ISSN 22782540 oct 2015.
17. Y. Zhang and W. Lee., " Intrusion detection in wireless ad hoc networks", In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pages 275-283, 2000.