International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 01 | Jan 2022 www.irjet.net p-ISSN: 2395-0072

Detecting Various Black Hole Attacks by Using Preventor Node in Wireless Sensor Networks

Ms. Shivani kushwaha [1], Mr. Anurag Jain[2], Mr. Rajneesh Pachouri[3]

[1]*M.Tech Research Scholar Department of Computer Science Engineering AIST, Sagar*
[2]*Assistant Professor, Department of Computer Science Engineering AIST, Sagar*
[3]*Assistant Professor, Department of Computer Science Engineering AIST, Sagar*

Abstract - *— S Security is a most important concern for MANET and attacker are extremely simply manipulated by the genuine performance and operation of the network. In this research project we provide a defense system against single black hole attacks and collaboratively at MANET. Blackhole attack drop packet attack behaves like a normal node during connection and after a false response sending location to the sender lowers all data packets. In this attack one or more than one malicious nodes create a secure environment with the presence of other continuously abut node exist in network and provides the secure communication in dynamic set-up. The attacker is only the nodes which are not forwarded packets to destination and also attacker/s is being a element of communication with each and every sender. The proposed IDS are not detect single black hole but also able to handle multiple black hole. The attacker nodes dropping are very harmful that dump actual presentation of network. The routing protocol is not able to defend the network from malicious activities. The black hole attacker is network layer routing attack and the projected plan is surely removes the attacker infection from the dynamic network and improves network performance .normal nodes. The proposed IDS (Intrusion Detection System) is identified the nodes those are not forwarded the data packets Key Words:*

Key Words: Keywords— Blac-khole, MANET, Routing, Security, IDS, Malicious nodes,

1. INTRODUCTION

Movable ad hoc network (MANET) is collection of wireless networks, which consists of huge number of mobile nodes. Nodes in moveable Ad hoc networks (MANET) can connect and leave the network dynamically. The mobility and scalability of MANET which does not have require of any permanent network infrastructure, makes it popular for different applications. So, it is extremely practical for emergency situation like military operation or disaster management. By means of definition, MANET is a group of itinerant nodes that performing functioning as the transmitter and receiver both communicate with each other via bidirectional link directly or indirectly mentioned in figure 1. Through RREQ request packets are flooded by sender and RREP reply packets are reverse back send to senders by receiver. The route selection for data sending is based on minimum hop count value. Therefore the path in between S-C-D is selected and rest of them is not selected for data sending in dynamic network.

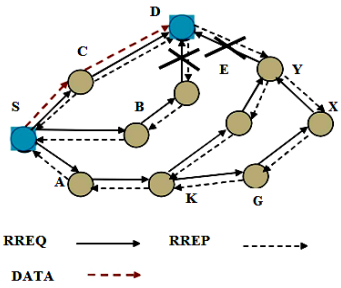

Figure 1 Network of Mobile Ad-hoc

MANET is an autonomous, self configuring network. This network can be deployed anywhere with ease without no support on any fixed infrastructure. There is infrastructure less and centralized administration in this type of networks. Nodes are constant from first to last wireless interface. The dynamic nature of such types of networks makes it very resistant to various link attacks. The essential requirements for a secured wireless networking are secure protocols which certify the discretion, availability, validity, truth of network. Many existing safety solutions for wire oriented networks are inefficacious and inefficient for Mobile ad hoc networks (MANET) environment. An network of ad hoc is the co-operative environment of a structure of mobile nodes which does not required an obstruction of any centralized system. An ad-hoc network is the temporarily established and created network, which is managed and operated by participating nodes. Network of Mobile Ad-hoc (MANET) is a group or set of changeable nodes which can contact to each other by using multi-hop wireless links. Mobile ad hoc network does not need any centralized management system and fixed network topology of nodes.

Mobile ad hoc network is spontaneous, infrastructure or topology less and self organized network. MANET has wide area use because of their self establishment, self creation, and self maintenance. Network of Mobile Ad-hoc (MANET) is an important part for communication for mobile system. Mobile system or nodes or device in the Network of Mobile Ad-hoc has a freedom for entry or exit from the network.

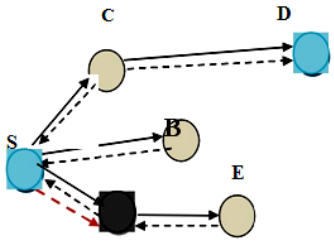

Figure 2 MANET Network Attack of Black Hole

2. Related Work

Related Work The previous work in field of black hole is mentioned in this section. These works are also efficient and provides information about the work is already done in field of attack.

In [6] Sathish M et.al proposed security scheme to protect the network from black hole attacks, it is important to discover malicious nodes during the route discovery process, when they pass fabricated RREP imitating the source node. The proposed methodology does precisely the same. Based on next hop information and destination sequence number that can be extracted from RREPs, this scheme handles particular and two-way black hole attacks with extenuated computational, routing and storage overhead.

In this work [7] V. Keerthika et.al proposed through/not direct trust is computed using normalized direction Reply misbehavior factor, link quality, and successful deliveries to moderate black hole attack. The hypothesis that node capability is also essential for efficient functioning of the network is not considered. In this work it is proposed to include network parameters to compute trust. Nodes travel a long distance in space among one in MANETs and are not specific of another's reliability because of not gathering sufficient evidence. The model is needed to represent uncertainty accordingly with common uncertainty.

In this paper [8] Raquel Lacuesta et.al can establish a secure self-configured environment for data distribution and resources and services sharing among users. A client is capable to connect the network because he/she knows somebody to facilitate belongs to it. Therefore the valid or certified authority is disseminated between the addicts that trust the new addict. The network management is also distributed.

In [10] Panthi N.K et. al. had proposed a scheme which not only substantiate the security of data but also guarantees the unremitting operation of negotiator by utilizing a dummy agent and composite acknowledgement technique. The network simulation also exemplify that no agent infertile for a few number of malicious nodes. Some weaknesses confirm the increase in delay, they have not considered the security of monitoring agent, and the processing time needed is also higher. They survey three approaches for the quandary of mobile agent protection. The three security approaches are preferred because each one is very uniquely implemented and has strengths that other approaches do not have to secure network. They opt for partial verification code because it can protect the results for mobile operators. Creating a computer with encrypted functions is preferred because it attempts to integrate code and data together. The blurry system approach is preferred because it confuses the agent code in such a way that no one can gain a complete understanding of its function.

In this paper [13] The NPV system is associated with high-level security structures. places advertised by its neighbors, and check their authenticity. They propose an NPV protocol with the following features

- It is deliberated for MANET dynamic or unpredictable environments, and as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes.

- It leverages cooperation but allow nodes to perform all substantiation events autonomously. This scheme has no need for extended connections, e.g., to reach a harmony among multiple nodes, making this scheme suitable for both low as well as high mobility environments.

- It is reactive, meaning that it can be executed by any node, at any point in time, without former awareness of the neighbourhood.

- It is vigorous besides independent and colluding adversaries. It is frivolous, as it generates low overhead traffic.

In [11], L.Tamilselvan et al., Suggests the view of the 'Fidelity Table. Here, every participating node is assigned a certain level of reliability, a measure of reliability. Whenever the sender code to the network broadcasts RREQ and raises, the received RREPs meet in their Response Table. If the reliability level of the RREP sending node (RREPN) and its subsequent hop node (NHN) route is found to exceed the pre-determined limit, RREPN is considered reliable. Therefore, in the adoption of multiple RREPs, those with the highest level of reliability are preferred. However, if multiple nodes have the same level of reliability, an RREP with a lower hop value is preferred. Finally, the route is accomplished in the selected way.

In this paper [14] Zhang et al. proposed a blackhole detection scheme based on sequence of number checking RREP packets. They consider the situation where the middle node is the attacker and suggest that, whenever the node sends RREP back to the source node, the middle node should also apply a sequence number to the destination. The destination node responds by sending a packet containing its sequence number to the source node. The source node then checks the freshness of the route by comparing the sequence number of the RREP received from the intermediate node (suspect) with the sequence number reply packet from the destination node; it consequently detects an attack if the

comparison fails. However, the beginning of two fresh packets with every response not only expands the overhead but also the nodes should make sure that the attacker does not drop or change these message sequence requests.

In this paper [20] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, Jiann-Liang Chen, CBDS Proposed: Co-Acquisition Acquisition Team is to stop the malicious activities of invading nodes of -MANET based on a mixed protection design. Provide a way to detect malicious nodes that trigger a blackhole or grayhole attack as well as a regional co-operation, known as the Cooperative Bait Detection (CBDS) theme. It integrates active and active defense structures, and randomly interacts with the nearest random node. By making the victim a node addresses nearby because it is the destination address, it eats malicious nodes to respond to RREP and identifies malicious nodes with the proposed tracking system and thus prevents its invasion.

In this research paper [22], the rejection of Service attacks is applied to the network; Evidence is collected to design an engine that detects the intrusion of the MANET Access System (IDS) system. There is a Feature Release and import rules are used to determine the accuracy of the acquisition engine using a vector support (SVM) machine. In this paper True affirmative formed by the detection engine. In this model True positive will be reported very quickly in Lids & Friend list that is generated by Lids will be sent to the Gids module for further analysis. According to trust level, The Universal Detection Engine will generate the friend list, higher the trust level of the node may be used for other different processes related to routing, and deciding the cluster head for scalable ad-hoc networks. Aspect takes out for the Routing parameters and MANET Traffic generation parameters can be used for different-different routing protocols. For the detection engine machine learning algorithm Support Vector Machine (SVM) is used which is light weighted.

3. Problem Statement

The attacker in MANET is degrades the routing performance. As we know that the behavior of attacker are of two types First is active attacker and other kind of attack is passive attacker. The reflexive attackers are not very unsafe for the communication but these attackers are drop only some amount of packets in network. The active attacker is very harmful for communication because it continuously targets the data packets in network.

The active attacker is very harmful for communication because it continuously targets the data packets in network. The black hole attacker is active attack and their presence in network is very harmful. The multiple attacker presence is more dangerous than single attacker presence because multiple attacker presence is cover the all normal nodes communication and drop the valuable data of senders. In MANET normal nodes are not possible to identify the black hole attacker presence in network. The attacker presence in network is drop the data packets is huge quantity because of that the packet receiving is reduced and also the throughput performance of network is minimized. The performance of end to end TCP and UDP protocol is also affected.

4. Proposed Work

The attacker presence in network is sure performing malicious activities in dynamic network. In MANET attack invaders easily enter the network and react like normal nodes. Malicious activity occurs during communication The attacker or attackers are being the element of network and this attacker presence is degrades the network performance.. In this study it is proposed to find a single black hole and multiple methods for the detection of black holes.

The proposed scheme is identified the attacker and also attackers in dynamic network through malicious profile of attacker. The attacker profile is different from the other normal nodes profile and also the attacker behavior is to not forward the data packets to actual destination. The attacker is drop these data packets in network. The behavior of attacker is identified through creating the routing mismanagement. This mismanagement entry is present in the attacker profile. The proposed algorithm is shows the recognition and prevention of single black hole attacks as well as attacks of multiple black holes separately on a dynamic network. The blocker is able to detect the malicious actions of the attacker on the network. The infection in the network is counted by preventer nodes because these nodes are actually confirming the attacker presence. Algorithm:

Algorithm: Algorithm: Single Black hole node discovery and prevention

Input:

M: mobile nodes

I: intermediate nodes

B: blackhole node

P: preventer node

S: Source node

D: destination node

rp: : routing packet ack: acknowledge

Seq: higher sequence number

AODV: routing protocol

Ψ: radio zone 550m

Output: blackhole node detection, percentage of infection, PDR, NRL, throughput

The same procedure with multiple preventer nodes is applied on multiple attackers. These attackers are very harmful because they are covering the whole network area and due to that the drooping and infection of attacker is more in network. The preventer nodes quantity is decided on the basis of cover all the malicious nodes in network. If the node density is high then in that case it is necessary to enhance the quantity preventer nodes also

5. Results and Discussion

The attacker aim is only to drop the information packets in network. These data packets are contain the valuable information of sender. The attacker is intermediate node behaves like a usual node in network and this node presence is loss the huge number of information packets in network.

Table 1 Black hole Node Identification and Data Loss Analysis

Node identification in 30 Nodes Scenario with data Loss

Attacker Node	Total Non-Authentic Packets
9	380

Node identification in 60 Nodes Scenario with Data Loss	
13	2255
17	6
29	1358
34	758
39	598

Summarized Performance Analysis

The summarized performance of network in presence of attacker and IDS is mentioned in table1. In this table the separate performance of two different scenarios of node 30 (single black hole) and node 60 (multiple black hole) are evaluated up to end of simulation time.

In this performance the attacker presence is clearly represents the huge loss of data in network due to packet capturing by attacker. The delay in presence of attacker is minimum because fewer amounts of packets are received at destination and only the delay measurement is count on the basis of packets are received at destination.

PDR Performance Analysis

The Packet Deliver Ratio (PDR) is actually represents percentage amount of data in network in presence of attacker and IDS. The number of packets in presence of multiple black hole attack is dropped more in network as compare to single black hole attack in network. PDR Performance Analysis The Packet Deliver Ratio (PDR) is actually represents percentage amount of data in network in presence of attacker and IDS. The number of packets in presence of multiple black hole attack is dropped more in network as match up to to single black hole attack in network. The PDR % in presence of single black hole attacker is about reaches to 84% and last value of PDR is recorded up to 70% at time about 30 seconds.

After that not a single packet is received at destination. In case of multiple black hole PDR value is counted up to end of simulation but negligible. The proposed IDS is blocked the malicious activities in network and provides secure routing performance in dynamic network. In both the cases IDS is effective and also use multiple IDS nodes in presence of multiple attackers is network

Table 2 Summarized Performance Analyses

Metrics	Performance in 30 nodes Scenario (Single Black hole)	Performance in 30 nodes Scenario (Multiple Black hole)	Performance in 60 nodes Scenario (Single Black hole)	Performance in 30 nodes Scenario (Multiple Black hole)
Send	2609	7034	5477	8218
Receive	551	7	5352	7643
Packet Capture	380	4975	0	0
PDR	21.12	0.1	97.72	93
NRL	4.34	512.57	0.31	0.52
Average E-E Delay(Ms)	73.5	51.5	254.91	454.37
Data Packets Dropped	2058	7027	125	575

6. Conclusion and Future Scope

The single attacker node presence is harmful for network then the multiple blackhole effect is really more harmful for network. The same malicious function is performed by other attacker nodes by that packet dropping is improves and whole network are easily covered by

attackers for injecting more infection. For improving network performance, we provides the reliable security scheme on the basis of packet dropping behavior of nodes in network. This research is very useful in field of security to evaluate the network performance in case of attack and IDS. The attack in MANET is easily loss the data and degrades the network routing performance. The previous work is provides the idea about how the different security scheme is apply the proper procedure to secure MANET routing performance.

The attacker presence is loss all data of network only some data is possible to deliver in destination in particular simulation time. The proposed IDS is recognized the behavior of blackhole attack by dropping property of attacker and also their presence is one hop count distance from sender. The proposed IDS behavior is maintain consistency for watching network behavior. The number of malicious nodes quantity is also identified by same packet dropping behavior. The simulation of network is performance in 30 nodes and 60 nodes. In both the scenario attacker effect is really terrible but after applying IDS attacker effect is controlled and also blocked by IDS in network. The presentation of network is improves applying proposed security scheme that improves PDR, throughput and minimizes packet dropping in network.

In this scheme the detection is based on RSS (Received Signal Strength) of mobile node and if node is drop packets then their RSS is week. Now check the reliability of node on the basis of packet dropping. The blackhole attacker is packet dropping attacker and other attacks like Tunnel attack is also the packet dropping attacker in dynamic network. In future we proposed the novel security scheme against Tunnel attack. The planned scheme is also applied on tunnel attack in MANET.

REFERENCES

1. Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials 15, no. 4 (2013): 2046-2069.

2. Pelechrinis, Konstantinos, Marios Iliofotou, and Srikanth V. Krishnamurthy. "Denial of service attacks in wireless networks: The case of jammers." IEEE Communications Surveys & Tutorials 13, no. 2 (2011): 245-257.

3. Yan, Qiao, F. Richard Yu, Qingxiang Gong, and Jianqiang Li. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges." IEEE Communications Surveys & Tutorials 18, no. 1 (2016): 602-622.

4. Huang, Qiang, Johnas Cukier, Hisashi Kobayashi, Bede Liu, and Jinyun Zhang. "Fast authenticated key establishment protocols for self-organizing sensor networks." In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pp. 141-150. ACM, 2003.

5. Latif, Rabia, Haider Abbas, and Saïd Assar. "Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review." Journal of medical systems 38, no. 11 (2014): 128.

6. Lupu, Teodor-Grigore, I. Rudas, M. Demiralp, and N. Mastorakis. "Main types of attacks in wireless sensor networks." In WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering, no. 9. WSEAS, 2009.

7. Gill, Khusvinder, and Shuang-Hua Yang. "A scheme for preventing denial of service attacks on wireless sensor networks." In Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE, pp. 2603-2609. IEEE, 2009.

8. Shamshirband, Shahaboddin, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." Engineering Applications of Artificial Intelligence 32 (2014): 228-241.

9. Yu, Yanli, Keqiu Li, Wanlei Zhou, and Ping Li. "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures." Journal of Network and computer Applications 35, no. 3 (2012): 867-880.

10. Modares, Hero, Rosli Salleh, and Amirhossein Moravejosharieh. "Overview of security issues in wireless sensor networks." In Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on, pp. 308-311. IEEE, 2011.

11. Shamshirband, Shahaboddin, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." Engineering Applications of Artificial Intelligence 32 (2014): 228-241.

12. Arunmozhi, S. A., and Y. Venkataramani. "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks." arXiv preprint arXiv:1106.1287 (2011).

13. Nanda, Rohan, and P. Venkata Krishna. "Mitigating denial of service attacks in hierarchical wireless sensor networks." Network security 2011, no. 10 (2011): 14-18.

14. Jan, Mian, Priyadarsi Nanda, Muhammad Usman, and Xiangjian He. "PAWN: a payload-based mutual authentication scheme for wireless sensor networks." Concurrency and Computation: Practice and Experience (2016).

15. ELBeltagy, Maha, Sarah Mustafa, Jariya Umka, Laura Lyons, Ahmed Salman, Chur-Yoe Gloria Tu, Nikita Bhalla, Geoffrey Bennett, and Peter M. Wigmore. "Fluoxetine improves the memory deficits caused by the chemotherapy agent 5-fluorouracil." Behavioural brain research 208, no. 1 (2010): 112-117.

16. Misra, Sudip, P. Venkata Krishna, Harshit Agarwal, Antriksh Saxena, and Mohammad S. Obaidat. "A learning automata based solution for preventing distributed denial of service in Internet of things." In Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, pp. 114-122. IEEE, 2011.

17. Shamshirband, Shahaboddin, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." Engineering Applications of Artificial Intelligence 32 (2014): 228-241.

18. Kumar, P. Arun Raj, and S. Selvakumar. "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems." Computer Communications 36, no. 3 (2013): 303-319.

19. Baig, Zubair A. "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks." Computer Communications 34, no. 3 (2011): 468-484.

20. Li, Shancang, Lida Xu, Xinheng Wang, and Jue Wang. "Integration of hybrid wireless networks in cloud services oriented enterprise information systems." Enterprise Information Systems 6, no. 2 (2012): 165-187.

21. Ho, Jun-Won, Matthew Wright, and Sajal K. Das. "Distributed detection of mobile malicious node attacks in wireless sensor networks." Ad Hoc Networks 10, no. 3 (2012): 512-523.

22. Hamdi, Mohamed, and Noureddine Boudriga. "Detecting Denial-of-Service attacks using the wavelet transform." Computer Communications 30, no. 16 (2007): 3203-3213.

23. Delgado-Mohatar, Oscar, Amparo Fúster-Sabater, and José M. Sierra. "A light-weight authentication scheme for wireless sensor networks." Ad Hoc Networks 9, no. 5 (2011): 727-735.

24. Vasserman, Eugene Y., and Nicholas Hopper. "Vampire attacks: draining life from wireless ad hoc sensor networks." IEEE transactions on mobile computing 12, no. 2 (2013): 318-332.

25. Redwan, Hassen, and Ki-Hyung Kim. "Survey of security requirements, attacks and network integration in wireless mesh networks." In New Technologies, Mobility and Security, 2008. NTMS'08., pp. 1-5. IEEE, 2008.