AN INTEGRATED ATTACK DISCOVERY AND DATA PROTECTION FRAMEWORK FOR MANET

Ms. S. Bharathi¹ and Mrs. M. Jothilakshmi²
¹PG & Research, Department Of Computer Science, Vivekanandha College of Arts & Sciences for Women (Autonomous), Namakkal-637 205, Tamil Nadu, India
²Asst. Professor, Department of Computer Science, Vivekanandha College of Arts & Sciences for Women (Autonomous), Namakkal-637 205, Tamil Nadu, India

Abstract-The mobile ad-hoc networks are build to support data transmission over infrastructure less environment. The Adaptive On-demand Distance Vector (AODV) routing protocol performs the route discovery operation when the source node initiates the route request. The malicious nodes drip out the route request packets and send false route reply information. Single or multiple black hole attacks are raised during the route discovery process. The black hole discovery process is carried out with the hybrid technique using fake route request and adjacent node verification based black hole node list preparation mechanism. The integrated attack discovery framework is build to detect the black hole, gray hole and worm hole attacks. Single and collaborative attack discovery process is supported in the framework. The coordinated attack discovery algorithm is developed to detect and control the Denial of Service (DoS) attacks. Trust and digital signature based protection mechanism is employed to control attack activities. The digital signed route request, path node trust assignment and RSA algorithm based security features are combined to ensure the attack prevention operations. The system is also focused to reduce the end to end delay with high throughput levels.

Keywords- Adaptive On-Demand Distance Vector (AODV) protocol, Black Hole Attacks, Gray Hole Attacks and Worm hole Attacks, Denial of Service (DoS) attacks and Cooperative Attack Detection Scheme

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is defined as the cooperative engagement of a collection of mobile nodes, without the support of any centralized access point or existing infrastructure. In this multi hop routing scenario, each node functions as a host and a router. Thus nodes are collectively responsible for network management. MANET has numerous applications in military and rescue zones since it gives an adaptable communication technique where geographical or terrestrial constraints are present [5].

Ad hoc distance vector routing is a reactive routing protocol in MANET that offers low processing and memory overhead, quick adaptation to dynamic link conditions and low network utilization. The paucity of security contemplation in the design of AODV makes it vulnerable to black hole attacks. In single black hole attack, a malicious node claims to have freshest and shortest route to destination, attracts data packets and drops them instead of forwarding. Sometimes these malicious nodes act in coordination resulting in collaborative black hole attacks. In this paper, we propose a novel solution to detect single and collaborative black hole attacks with reduced computational, routing and storage overhead.

This strategy makes use of fake route request, destination sequence number and next hop information to identify the malicious nodes.
II. ATTACKS IN MANET

Recently, ad hoc networks have been gaining popularity for applications requiring quick deployment. Researchers have tried to propose protocols that will improve the quality of service for ad hoc networks in the hostile wireless environments. Many of the applications, particularly military applications, require a high level of security. Thus, the main challenge is to protect ad hoc networks from security attacks. As ad hoc networks use the open wireless medium to communicate, it makes easy for an attacker to launch attacks by injecting, blocking, or modifying the packets. All the nodes act as routers for the data packets and there is no clear line of defense where it is possible to place a firewall-like device.

Blackhole attack concerns with the network layer of MANET. In black hole attack, an attacker or malicious node aims to consume all the data packets throughout the network. Black hole attack can be of different types depending on aims of the attacker after interception of data exchange between other nodes. Depending on black hole type, after interception of data exchange attacker can either drop all the packets or it can selectively drop packets, or even the malicious node can modify the packets.

A gray hole attack is a variation of black hole attack, where an adversary first behaves as an honest node during the route discovery process, and then silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. Detection of grayhole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature.

In ad hoc networks one of the most challenging attacks to defend against is the wormhole attack. In wormhole attack, the attacker replays the data and control packets from one location in the network to another location. The two locations are several hops away from each other, but well connected through a high-speed wired or wireless link controlled by the attacker. The goal of the attacker is not to improve the network connectivity but to draw traffic through the wormhole and disrupt routing.

Denial of Service (DoS) a malicious node may generate frequent unnecessary routing requests to make the network resources unavailable to other nodes. DoS attack results when the network bandwidth is hijacked by a malicious node. A malicious node may impersonate another node while sending the control packets to create an anomaly update in the Routing Table (RT).

III. RELATED WORK

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative blackhole attacks. In addition, some of these methods require specific environments [10] or assumptions in order to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories. 1) Proactive detection schemes [6], [8] are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. One of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage. 2) Reactive detection schemes are those that trigger only when the destination node detects a significant drop in the packet delivery ratio.

Among the above schemes are the ones proposed, which we considered as benchmark schemes for performance comparison purposes. Liu et al. proposed a 2ACK scheme for the detection of routing misbehavior in MANETs [9]. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received. A parameter acknowledgment ratio, i.e., Rack, is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to the class of proactive schemes and, hence, produces additional routing overhead regardless of the existence of malicious nodes. Xue and
Nahrstedt proposed a prevention mechanism called best-effort fault-tolerant routing (BFTR). Their BFTR scheme uses end-to-end acknowledgements to monitor the quality of the routing path to be chosen by the destination node. If the behavior of the path deviates from a predefined behavior set for determining “good” routes, the source node uses a new route. One of the drawbacks of BFTR is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, which may lead to significant routing overhead. Our proposed detection scheme takes advantage of the characteristics of both the reactive and proactive schemes to design a DSR-based routing scheme able to detect grayhole/collaborative blackhole attacks in MANETs.

IV. BLACK HOLE ATTACK DISCOVERY IN MOBILE AD-HOC NETWORKS

Mobile Ad-hoc NETwork (MANET) owing to its inherent properties has gained a lot of recognition in the field of communication [1]. MANET is a self-organized set of wireless connections to build up a network of mobile or movable nodes [3]. The mobile nodes in MANET communicate without the presence of a permanent infrastructure and the transmission links are also established through wireless medium and does not entail a centralized command and control from any node. [4].

Contemporary military requirements and battlefield scenario presses upon equipping the military’s ground soldier with latest communication technology equipment. MANETs are considered eminent resources and endow efficient means of communication to military. It can integrate and provide real time information of battlefield to Command Control Communication and Information System (C3IS), troops, vehicles and tanks operating in the conventional operation or battlefield especially when operating inside enemy territory, offensive operations or Counter Insurgency/Counter Terrorism operations beyond the reach of a permanent network infrastructure. Inclusion of communication equipments based on this MANET gives an added advantage over our foes and strengthens our communication infrastructure by enabling swift communication at our disposal. Main concern is security of network, as military applications necessitate use of high level of security infrastructure.

Since security being an essential criterion in military for both the wired and wireless network communication, success of a MANET is based prominently on whether the infrastructure is secure or not. The routing protocols which were developed for MANET, lack defensive procedures and are thus vulnerable to a number of attacks [2]. These traits of MANET set the demands and possibilities for achieving the important security goals. Some attacks can mark some particular routing protocols as their targets for example AODV. Security attacks such Single and cooperative Black Hole attacks have been portrayed in few publications and research papers. Presently, security in routing protocols is one of the trending research areas in MANET.

Black hole attack being an important denial of service attacks which when set off by malicious nodes, reduces network performance [7]. If there exist more than one black hole nodes present in the network, the malicious nodes can be used for activating a black hole attack called multiple/cooperative black hole attack.

V. SECURITY ISSUES ON MANET DATA COMMUNICATION

The Adaptive On-demand Distance Vector (AODV) routing protocol performs the route discovery operation based on source node request. The malicious nodes drip out the route request packets and send false route reply information. Single or multiple black hole attacks are raised during the route discovery process. The black hole discovery process is carried out with the hybrid technique. The hybrid technique prepares and transmits the black hole node list to other nodes. The black hole node list is formed with fake route request and adjacent node verification process. Black Hole nodes are isolated with reference to the black hole node list data. The route request packets are not forwarded to
the nodes in black hole list. The following security issues are identified from the current MANET data communication schemes.

- Gray hole and worm hole attack discovery is not supported
- Attack prevention operations are not supported
- Denial of Service (DoS) attacks are not handled
- High end to end delay with low throughput levels

VI. AN INTEGRATED ATTACK DISCOVERY AND DATA PROTECTION FRAMEWORK

The integrated attack discovery framework is build to detect the black hole, gray hole and worm hole attacks. Single and collaborative attack discovery process is supported in the framework. The coordinated attack discovery algorithm is developed to detect and control the Denial of Service (DoS) attacks. Trust, Cryptography and digital signature based protection mechanism is employed to control attack activities. The MANET data security system is build to handle attack discovery and prevention operations. Black hole, gray hole and worm hole attacks are discovered in the system. Trust, Cryptography and digital signature models are integrated in the system. The system is divided into five major modules. They are Data communication process, Attack discovery with hybrid technique, Collaborative attack discovery, Integrated attack discovery and Attack prevention process. The route discovery process is initiated in the data communication process. Single and multiple black holes are detected with hybrid technique. Attack groups are detected in the collaborative attack discovery process. Gray hole, worm hole and DoS attacks are discovered in the integrated attack discovery process. Trust and digital signature models are used in the attack prevention process.

The Mobile Ad-hoc networks are constructed with user specified area and node count levels. All the data communication operations are initiated with Adaptive On-demand Distance Vector (AODV) protocol. The route discovery process is initiated with route request process issued by the source node. The source node selects the route from the received route reply information. The black hole attack detection process is carried out using hybrid technique. Single and cooperative attack detection operations are combined in the hybrid technique. Fake route request and adjacent node verification operations are carried out to discover the black hole nodes. The black hole node list is broadcasted to all other nodes.

The collaborative attack discovery technique is applied to malicious node groups. The route reply information are verified under the source node for malicious node discovery process. Single black hole node list and collaborative black hole node list are prepared in the attack detection process. The collaborative black hole node list maintains the attacker group information. The gray hole, worm hole and black hole attacks are detected using integrated attack discovery mechanism. The Denial of Service (DoS) attacks are raised with malicious service requests. The coordinated attack discovery algorithm is used to discover the malicious nodes and attack activities. The malicious node details are transferred to all nodes for malicious node isolation process. Malicious node activities are controlled in the attack prevention process. Node trust assignment and verification is used to authorize the nodes in route discovery and data communication tasks. The route request and reply packets are secured with Cryptography techniques. Route request and reply packets are verified with digital signatures.

VII. EXPERIMENTAL ANALYSIS

The MANET attack detection process is build to discover the black hole, gray hole and worm hole attacks. The Hybrid Technique (HT) is applied to discover the single and cooperative black hole attacks. The Integrated Attack Discovery Technique (IADT) is build to discover and control the attacks. The system is performed with the three parameters. They are Attack detection ratio, Packet delivery rate and End to End delay Parameters.
Figure No. 7.1. Attack Detection Accuracy level analysis between Hybrid Technique (HT) and Integrated Attack Discovery Technique (IADT)

Figure No. 7.2. Packet Delivery Rate analysis between Hybrid Technique (HT) and Integrated Attack Discovery Technique (IADT)
The attack detection accuracy is analyzed with actual attacks and detected attack ratio levels. The accuracy level is measured with attack detection rate parameter. The Attack detection rate analysis between the Hybrid Technique (HT) scheme and Integrated Attack Discovery Technique (IADT) scheme is shown in figure 7.1. The Integrated Attack Discovery Technique (IADT) scheme increases the Attack detection rate 20% than the Hybrid Technique (HT) scheme. The packet dripping is the main challenge in the black hole, gray hole and worm hole attacks. The packet delivery rate measure is used to estimate the ratio between the total transmitted packets and total delivered packets. The Packet delivery rate analysis between the Hybrid Technique (HT) scheme and Integrated Attack Discovery Technique (IADT) scheme is shown in figure 7.2. The Integrated Attack Discovery Technique (IADT) scheme increases the Packet delivery rate 15% than the Hybrid Technique (HT) scheme. The data transmission and route request transmission time period is estimated in the end to end delay analysis. The time period for data and route details transmission is estimated as end to end delay measure. The end to end delay analysis between the Hybrid Technique (HT) scheme and Integrated Attack Discovery Technique (IADT) scheme is shown in figure 7.3. The Integrated Attack Discovery Technique (IADT) scheme reduces the End to End delay 20% than the Hybrid Technique (HT) scheme.

VII. CONCLUSION

Routing protocols are used to manage the data transmission process over the Mobile Ad-hoc Network (MANET) nodes. The hybrid technique is applied to detect single and cooperative black hole attacks. Black hole, gray hole and worm hole attacks are discovered with Single and collaborative attack detection scheme. The coordinated attack detection algorithm and node trust values are used to detect and control the attacks. The MANET attack discovery system is build to detect black hole, gray hole and worm hole attacks. Single and collaborative black hole attacks are discovered by the system. Route discovery delay is minimized with high throughput levels. Service request based attacks are also detected by the system.
REFERENCES

[1] Kriti Patidar, Vandana Dubey, “Modification in Routing Mechanism of AODV for Defending Black hole and Wormhole Attacks”, IEEE Conference on IT in Business, Industry and Government (CSIBIG), March 2014.
[2] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao and Chin-Feng Lai, Member, IEEE “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach” in proc IEEE systems journal, 2015.
[3] Pooja Jaiswal, Rakesh Kumar, “Prevention of Black Hole Attack in MANET” IRACST, International Journal of Computer Networks and Wireless Communications (IJCNCW), ISSN: 2250-3501 Vol.2, No5, October 2012.
[4] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal “Detection and Removal of Co-operative Black hole and Grayhole Attacks in MANETs” IEEE International Conference on System Engineering and Technology September 11-12, 2012, Bandung, Indonesia.
[5] Priyanka Goyal, Vinti Parmar, Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Applications”, International Journal of Computational Engineering & Management, Vol. 11, January 2011, 32-37.
[6] Baadache and A. Belmehdi, “Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks,” Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.
[7] Pradip M. Jawandhiya, Mangesh M Ghonge, M.S. Ali, J.S Deshpande, “A Survey of Mobile Ad hoc Networks” International Journal of Engineering Science and Technology, Vol. 2(9), 2010, 4063-4071.
[8] K. Vishnu and A. J Paul, “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,” Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.
[9] 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 Systems Journal, 2017.
[10] P.-C. Tsou, J.-M. Chang, H.-C. Chao and J.-L. Chen, “CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture,” in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011,3 pp. 1–5.