International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol.10 No.3 Jan – Feb 2023

A Study on Detect and Prevent Network strike in MANETS

Dr. Bhasker Gangadhar Koshidgewar
Head, Department of Computer Science Vai. Dhunda Maharaj Deglurkar College, Degloor Dt. Nanded (M.S)- INDIA
ORCID ID -2301056
***Corresponding Author*- Dr. Bhasker Gangadhar Koshidgewar**
E-mail id : bhasker149@gmail.com
DOI- 10.5281/zenodo.7583280

Abstract:
The greatest challenge for the MANETS is to come with a robust security solution even in the presence of malicious nodes, so that MANET can be protected from various routing strikes. Several countermeasures have been proposed for these routing strikes in MANETS using various cryptographic techniques. But most of these mechanisms are not considerably suitable for the resource constraints, i.e., bandwidth limitation and battery power, since they results in heavy traffic load for exchanging and verification of keys. In this paper, a new semantic security solution is provided, which suits for the different MANET constraints and also is robust in nature, since it is able to identify and prevent four routing strikes parallel.

Keywords: MANET, Security, Robust, Malicious nodes, Semantic security.

1. Introduction

A MANET has got some of the important properties like self organized and rapid deployable capability; which makes it widely used in various applications like emergency operations, battlefield communications, relief scenarios, law enforcement, public meeting, virtual class rooms and other security-sensitive computing environments [1]. There are several issues in MANETS which addresses the areas such as IP addressing, radio interference, routing protocols, power Constraints, security, mobility management, bandwidth constraints, QOS, etc;. As of now some hot issues in MANETS can be related to the routing protocols, routing strikes, power and bandwidth constraints, and security, which have raised lot of interest in researchers. Even though in this paper we only focus on the routing strikes and security issue in MANETS. The MANET security can be classified in to 5 layers, as Application layer, Transport layer, Network layer, Link layer, and Physical layer. However, the focus is on the network layer, which considers mainly the security issues to protect the ad hoc routing and forwarding protocols. When the security design perspective in MANETS is considered it has not got a clear line defense. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious strikeers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred. On the other hand, the existing ad hoc routing protocols, such as (AODV (Ad Hoc on Demand Distance vector protocol)) [2] [3], (DSR (Dynamic Source Routing)) [4], and wireless MAC protocols, such as 802.11 [5], typically assume a trusted and cooperative environment. As a result, a malicious strikeer can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications. Recently, several research efforts introduced to counter against these malicious strikes. Most of the previous work has focused mainly on providing preventive schemes to protect the routing protocol in a MANET. Most of these schemes are based on key management or encryption techniques to prevent unauthorized nodes from joining the network. In general, the main drawback of these approaches is that they introduce a heavy traffic load to exchange and verify

keys, which is very expensive in terms of the bandwidth-constraint for MANET nodes with limited battery and limited computational capabilities. The MANET protocols are facing different routing strikes, such as flooding, black hole; link withholding, link spoofing, replay, wormhole, and colluding misrelay strike. A comprehensive study of these routing strikes and countermeasures against these strikes in MANET can be found in [6] [1]. The main goal of the security requirements for MANET is to provide a security protocol, which should meet the properties like confidentiality, integrity, availability and non-repudiation to the mobile users. In order to achieve this goal, the security approach should provide overall protection that spans the entire protocol stack. But sometimes the security protocol may not be able to meet the requirements as said above and results in a packet forwarding misbehavior. That is why the approach proposed here is not coupled to any specific routing protocol and, therefore, it can operate regardless of the routing strategy used. The main criterion for identification of a malicious node is the estimated percentage of packets dropped, which is compared against a pre-established misbehavior threshold. Any other node which drops packets in excess of the pre-established misbehavior threshold is said to be misbehaving, while for those nodes percentage of dropping packets is below the threshold are said to be properly behaving. The approach proposed here identifies and prevents misbehaving nodes (malicious), which are capable of launching four routing strikes parallel: the black hole strike, wherein a misbehaving node drops all the packets that it receives instead of normally forwarding them. A variation of this strike is the gray hole strike, in which nodes either drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). The gray hole strikes of this types will anyhow disrupt the network operation, if proper security measures are not used to detect them in place [7]. A simple eavesdropping of packets strike and message tampering strikes are also identified and prevented by the proposed approach. The proposed approach is demonstrated through a practical experiment for an appropriate selection misbehaved and well-behaved nodes using a misbehavior threshold. We tested for the robustness of the approach against fixed node mobility in a network that is affected parallel by four strikes. The rest of this paper is organized as follows. Section II describes related work in the area of MANET security. Section III describes the proposed algorithm for packet forwarding misbehavior identification and prevention, and Section IV presents the experimental analysis and performance evaluation. Finally, the paper is concluded in Section V.

2. Related Work

Reliable network connectivity in wireless networks is achieved if some counter measures are taken to avoid data packet forwarding against malicious strikes. A lot of research has taken place to avoid malicious strikeers like, a Survey on MANET Intrusion Detection [8], Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks [9], Detecting Network Intrusions via Sampling : A Game Theoretic Approach [10], Collaborative security architecture for black hole strike prevention in mobile ad hoc networks [11], A Distributed Security Scheme for Ad Hoc Networks [6], Wormhole strikes detection in wireless ad hoc networks: a statistical analysis approach [12], Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks [13], Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks[7], WAP: Wormhole Strike Prevention Algorithm in Mobile Ad Hoc Networks [4], A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET [14], Secure Routing Protocol with Malicious Nodes Detection for Ad Hoc Networks (ARIADNE) [15], A Cooperative Black hole Node Detection Mechanism for ADHOC Networks [5], Malicious node detection in Ad Hoc networks using timed automata [16], Addressing Collaborative Strikes and Defense in Ad Hoc Wireless Networks [17], dpraodv: a dynamic learning system against black hole strike in aodv based manet [18], and Performance Evaluation of the Impact of Strikes on Mobile Ad hoc Networks [19]. All these research work reveals that a single or to a maximum of two or three strikes identification and prevention using some approach is considered. Our solution to this research gap is to provide a semantic security scheme that considers a minimum of 4 strikes identification and prevention parallel

using a simple acknowledgement approach. The above related study justifies that, the proposed scheme is not considered anywhere and is a new security solution for network layer strikes. The reason to concentrate on network layer strikes because; as we know a MANETS network connectivity is mainly through the link-layer protocols and network-layer protocols. The Link-layer protocols are used to ensure one-hop connectivity while network-layer protocols extend this connectivity to multiple hops [2]. So only to incorporate MANETS security we can consider two possible counter measures namely, link-layer security and network-layer security. Link-layer security is to protect the one-hop connectivity between two adjacent nodes that are within each other's communication range through secure protocols, such like the IEEE 802.11 WEP protocol [3] or the more recently proposed 802.11i/WPA protocol [20] [2]. The network-layer security mainly considers for delivering the packets between mobile nodes in a secure manner through multihop ad hoc forwarding. This ensures that the routing message exchange within the packets between nodes is consistent with the protocol specification. Even the packet forwarding of every node is consistent with its routing states. Accordingly, the protocols are broadly classified in to two categories: secure ad hoc routing protocols and secure packet forwarding protocols. The paper mainly discusses about the network-layer security.

3. Proposed Approach

The routing strikes like black hole, gray hole, worm hole, rushing strike, DOS strike, flooding etc; can become hazardous to the network-layer protocol which needs to be protected. Further the malicious nodes may deny forwarding packets properly even they have found to be genuine during the routing discovery phase. A malicious node can pretend to join the routing correctly but later goes on ignoring all the packets that pass through it rather than forwarding them. This strike is called black hole, or selective forward of some packets is known as grey hole strike. The basic solution needed to resolve these types of problems is to make sure that every node in a network forwards packets to its destination properly. To ensure this kind of security to network layer in MANETS a new secure approach which uses a simple acknowledgement approach and principle of flow conservation is proposed here. As a part of this research work we have tried the same approach with AODV protocol and it has identified two of the strikes namely message tampering and packet eavesdropping. Here, in this proposed work the same approach has been tested to identify more than two strikes in a network without the use of protocol. The related work in section 2 exactly reveals that there has been no approach till yet found to identify and prevent the network layer strikes parallel. This paper mainly concentrates on this part of the research and unveils that the more than one strike can be identified and prevented parallel independent of the protocol for routing. The design of the proposed algorithm is done based on three modules, namely the sender module, the intermediate node module and the receiver module. The approach is independent of the data forwarding protocol. To develop the proposed algorithm, a simple acknowledgement approach and principle of flow conservation have been applied. Conventions used for the algorithm development: The packet sending time by the source node will be start time. According to principle of flow conservation the limit of tolerance is set to some threshold value i.e. in this algorithm it will be 20%. The time taken for the acknowledgement to reach back the source is end time. The total time taken for transmission will be (end-start) = RTT (Round Trip Time). To count the packets sent a counter Cpkt is used. The RTT time limit is set to 20 milliseconds. When an acknowledgement that is received by the sender exceeds the 20 ms time limit, then the data packet will be accounted as a lost packet. To count the number of lost packets another counter Cmiss is used. The ratio of (Cmiss/Cpkt) is calculated. If the ratio calculated exceeds the limit of tolerance threshold value 20%, then the link is said to be misbehaving otherwise properly behaving. Parallel using the ratio value, the corresponding strikes will be identified. The algorithm is explained as follows: The sender node module generates the front end and asks the user to enter the message. The user enters the messages or browses the file to be sent and clicks on send button. The counter Cpkt gets incremented every time a packet is sent and the time will be the start time. According to the data format only 48 bytes are sent at a time. If the message is longer than 48 bytes then it is divided into packets

each of 48bytes. For maintaining intact security in the algorithm a semantic mechanism like one-way hash code generation to generate the hash code for the message is used. For generating hash code hash function is applied in the algorithm. A hash function is an algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message. The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or simply digests. Sender module then prepares the data frame appending the necessary fields namely source address, destination address, hash code and data to be sent. Then the data packets will be sent to nearest intermediate nodes. On receiving the message at the intermediate node, a choice will be made available at the nodes module to alter or not to alter the data and the intermediate node behaves accordingly. Then the intermediate node finds the destination address in the data frame and forwards data to it. Once the receiver receives the message, it extracts the fields from the data frame. These extracted fields are displayed on to the front end generated by the receiver module. The receiver also computes the hash code for the message received using the same hash function that was used at the sender. The receiver compares the hash code that was extracted from the data frame with the hash code that it has generated. An accidental or intentional change to the data will change the hash value. If the hash codes match, then the acknowledgement packet sent back to the sender through the intermediate node consists of “ACK”. Else when the hash codes do not match the acknowledgement packet sent back to the sender through the intermediate node consists of “CONFIDENTIALITY LOST”. At the sender node, the sender waits for the acknowledgement packet to reach. Once it receives the acknowledgement packet it computes the time taken for this acknowledgement to reach I.e. the end time. If the total transmission time taken I.e. (end-start) is more than the pre-specified interval of 20 ms, it discards the corresponding data packet and accounts it as lost data packet, thereby incrementing the Cmiss counter. Else it checks for the contents of acknowledgement field. If the ratio of (Cmiss/Cpkt)>=20%, then the intermediate node is said to be misbehaving and a new field “CONFIDENTIALITY LOST” is built in to the acknowledgement frame. In such a case, sender switches to an alternate intermediate node for the future sessions. Otherwise another new field “ACK” is built in to the acknowledgement frame. In this case the intermediate node is considered to be behaving as expected and transmission is continued with the same intermediate node. Such intermediate nodes can be called genuine nodes. Simultaneously malicious nodes are identified and prevented which launch strikes. The algorithm mainly identifies four strikes parallel namely packet eavesdropping, message tampering, black hole strike and gray hole strike. This reason makes the algorithm more robust in nature against other approaches. Even it can also be extended to few more network layer strikes.

The strikes explanation is as follows:

1.***Packet eavesdropping*:**

In mobile ad hoc networks since nodes can move arbitrarily the network topology which is typically multi hop can change frequently and unpredictably resulting in route changes, frequent network partitions and possibly packet losses. Some of the malicious nodes tend to drop packets intentionally to save their own resources and disturb the network operation. This particular strike is identified by the value of the (Cmiss/Cpkt) ratio. If (Cmiss/Cpkt)>20%, them link contains a malicious node launching packet eavesdropping strike.

2. *Message tampering:*

The intermediate nodes sometimes don’t follow the network security principle of integrity. They will tend to tamper the data that has been sent either by deleting some bytes or by adding few bytes to it. This strike can be an intentional malicious activity by the intermediate nodes. The algorithm identifies such nodes and strike by the value of the ratio calculated for different data transmissions. If the acknowledgement frame sent by the receiver contains “CONFIDENTIALITY LOST” field in it, then the node is said to be tampered the data sent. Along with that if the ratio (Cmiss/Cpkt)>20%, then link is said to be

misbehaving and message tampering strike is identified.

3. *Black hole strike:*

In this strike a misbehaving node drops all the packets that it receives instead of normally forwarding those [2]. The routing message exchange is only one part of the network-layer protocol which needs to be protected. It is still possible that malicious nodes deny forwarding packets correctly even they have acted correctly during the routing discovery phase.

For example, a malicious node can join the routing correctly but simply ignore all the packets passing through it rather than forwarding them, known as black hole strike [. In a blackhole strike, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.

For example, in AODV, the strikeer can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This cause the source node to select the route that passes through the strikeer. Therefore, all traffic will be routed through the strikeer, and therefore, the strikeer can misuse or discard the traffic [1]. This strike is identified if the ratio (Cmiss/Cpkt)>=1.0, then all the sent packets are said to be lost or eavesdropped by the malicious node.

4. *Gray hole strike*:

A variation of the black hole strike is the gray hole strike [7]. This strike when launched by the intermediate nodes selectively eaves drop the packets I.e. 50% of the packets, instead of forwarding all. This strike is identified if the ratio (Cmiss/Cpkt)>0.2 and (Cmiss/Cpkt) = 0.5, then we can say half of the packets that have been sent are eaves dropped by the malicious node.

4. Experimental Analysis

The proposed algorithm was practically implemented and tested in a lab terrain with 24 numbers of nodes in the network. Through the experiment analysis it is found that the algorithm exactly shows the results for four strikes parallel namely packet eaves dropping, message tampering, black hole strike and gray hole strike. To analyze the semantic security mechanism, two laptops are connected at both the ends in between 22 numbers of intermediate nodes with WI-FI connection.The data pertaining to the lab records are, the underlying MAC protocol defined by IEEE 802.11g with a channel data rate of 2.4 GHZ. So only the approach is more economic in nature and it can be considered as more robust in nature, since it is able to identify and prevent four strikes parallel in MANETS. The same algorithm can be extended to few more network layer strikes identification and prevention, which can be taken as the future enhancement. Further the network density can also be increased and using the proposed approach it can be tested and analyzed. Simulation can also be taken as another enhancement for the approach to consider more number of nodes and graphical analysis.

4.1. Performance Analysis

We have considered four of the network parameters for evaluating the performance with the proposed approach. Further it can be extended to a few more parameters based upon the network density. The algorithm can also be extended to identify and prevent few more network layer strikes. Another important fact can be considered with respect to the approach is the power consumption of the nodes in the network. When compared to other approaches, the proposed scheme presents a simple one-hop acknowledgement and one way hash chain, termed as semantic security mechanism, greatly reduces overhead in the traffic and the transmission time. The overall transmission for sending and receiving data happens in just few milliseconds, overcoming the time constraint thereby reducing power consumption. As a part of the analysis, the proposed approach which is a protocol less implementation is compared with the protocol performances like AODV and DSR. Only one network parameter i.e. throughput has been taken for comparison with increasing the number of nodes up to 24.

5. Conclusion And Future Work

In mobile ad hoc networks, protecting the network layer from strikes is an important research topic in wireless security. This paper describes a robust scheme for network-layer security solution in ad hoc networks, which protects both, routing and packet forwarding functionalities without the context of any data forwarding protocol. This approach tackles the issue in an efficient

manner since four strikes have been identified parallel. The overall idea of this algorithm is to detect malicious nodes launching strikes and misbehaving links to prevent them from communication network. This work explores a robust and a very simple idea, which can be implemented and tested in future for more number of strikes, by increasing the number of nodes in the network. To this end, we have presented an approach, a network-layer security solution against strikes that protects routing and forwarding operations in the network. As a potential direction for future work, we are considering measurement of more number of network parameters, to analyze the performance of such a network using the proposed approach.

6. References

[1] Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala. "*A Review of Current Routing Strikes in Mobile Ad hoc Networks*". Inte. Journal of Computer Science and Security, 2(3):18-29, 2008

[2] Bingwen He, Joakim Hägglund and Qing Gu. "*Security in Adhoc Networks*", An essay produced for the course Secure Computer Systems HT2005 2005

[3] IEEE Std. 802.11. "*Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications*", 1997

[4] Sun Choi, Doo-young Kim, Do-hyeon Lee and Jae-il Jung. "*WAP: Wormhole Strike Prevention Algorithm In Mobile Ad Hoc Networks*", In Proceedings of International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Vol. 0, ISBN = 978-0-7695-3158-8, pp. 343-348, 2008

[5] Moumita Deb, "*A Cooperative Black hole Node Detection Mechanism for ADHOC Networks*", Proceedings of the World Congress on Engineering and Computer Science, 2008

[6] Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia, Nirali Mody, Sugata Sanyal and Ajith
Abraham. "*A Distributed Security Scheme for Ad Hoc Networks*", ACM Publications, Vol-11, Issue 1, pp.5–5, 2004