American Journal of Electrical and Computer Engineering
2018; 2(1): 1-4
http://www.sciencepublishinggroup.com/j/ajece
doi: 10.11648/j.ajece.20180201.11

A Survey on Game Theory Approaches for Improving Security in MANET

Rahul Krishnan

Department of Electronics and Communication Engineering, Rajalakshmi Institute of Technology, Chennai, India

Email address:
rahulkrish1990@gmail.com

To cite this article:
Rahul Krishnan. A Survey on Game Theory Approaches for Improving Security in MANET. *American Journal of Electrical and Computer Engineering*. Vol. 2, No. 1, 2018, pp. 1-4. doi: 10.11648/j.ajece.20180201.11

Received: May 2, 2018; **Accepted**: May 29, 2018; **Published**: June 12, 2018

Abstract: The MANET is the most widely used networks due to the usage of wide range of multimedia applications over the wireless networks. One of the main features of nodes in mobile ad hoc networks (MANETs) is their collaboration with neighbors to propagate data. Exploiting this feature, malicious nodes collaborate with normal nodes to disturb network operation and reduce its efficiency. These nodes attack other network nodes and avoid being detected by other nodes through using the mobility characteristic of nodes in MANETs. Because of the infrastructure less network, battery constraint and the non-cooperative environment it is difficult to provide security to the network. Some nodes try to save their energy and start to exhibit malicious activities like dropping the packet by not forwarding etc. Due to such security problems in the network, the routing also becomes inefficient. Hence to improve the routing efficiency along with security, several techniques have been used so far. One of the effective ways to detect malicious nodes is using game theory. In this work, several such routing techniques have been compared and analyzed and a survey has been made. The different kinds of security attacks have been analyzed and the proposed solutions have been tabulated in this survey.

Keywords: MANET, Malicious, Route Request, Route Reply, Authentication

1. Introduction

The communication was originally started with wired networks through physical medium that last longer for several decades. Later the communication was made through the wireless medium where physical medium was not needed. These wireless networks are then transformed into another form where the nodes of the network move constantly and this type of network was termed as Mobile networks. In these mobile networks, a new challenge for routing arouses which is called Mobile Ad-hoc Network where the topology changes dynamically. Mobile ad hoc networks are comprised of a collection of dynamic cooperating nodes which are connected with each other by wireless technologies. These nodes may join and leave the network at any time. The information transfer in this network is done in multi-hop fashion. Hence collaboration between the nodes is the most important factor for transferring information.

We are living in the age where information is an asset. When the information is passed, it should reach the destination without being attacked. Hence the data should be hidden from confidentiality, integrity and availability. The attacker can absorb the network traffic and injects themselves in the path to attack the information. As there is no fixed infrastructure in MANET, there is no any dedicated part for each specifying functionality. It is a difficult task to provide security to MANET due to its mobile nature, lack of centralized monitoring, and limited resources like battery power and bandwidth. Since there is no specified infrastructure, the network is more prone to the invasion of malicious nodes. These malicious nodes harm the network and retract the nodes from data forwarding. Hence, proper secure routing mechanisms must be used in the network to avoid such misbehaviors.

There are several routing mechanisms available for routing in MANET such as AODV, CGSR, DSDV, GSR, FSR, OLSR etc. But these techniques are not assured in enhancing security. Hence to provide increased security with efficient routing, several techniques have been designed. Some of those techniques are ARAN, SAR, SEAD, ARIADNE, SLSP, SAODV, CORE, CONFIDANT etc. The network should be secured from the malicious intruders so that by avoiding such

nodes in the network, routing also can be done efficiently with only regular nodes.

In this paper, a survey has been made on several security issues and various attacks that can be made on the MANET and the proposed solutions to those problems. The first section describes about the security targets and the second section describes about the possible attacks on network and the last section provides the proposed solutions for those attacks.

2. Security Target

The routing in MANET while transmitting the data should be secured. The main goals of providing security to the network are based on few parameters which should be meet out. These security service parameters are nearly similar to that of the other wired or any infrastructure wireless networks.

2.1. Authentication

All the nodes in the network that involves transmission should be properly authenticated. If any node is not authenticated, then it can act malicious node that invades the network to affect the transmission of data packets between the nodes. Hence all the nodes in the network should be authenticated.

2.2. Availability

Availability ensures that the service in the network exists even during attacks. The service should be available in the network whenever they are needed. Various attacks in the network such as denial of services, energy starvation attacks and node behavior can be taken care of by the network if they ensure availability.

2.3. Confidentiality

This confidentiality ensures that the private information about the nodes and the data should be accessible only by the intended nodes. The nodes that hop the information from sender to receiver nodes should not be accessible to the information. The encryption of data greatly helps in ensuring confidentiality of the information.

2.4. Integrity

The Integrity ensures that the data that is transmitted should not be modified by any other intermediate nodes.

2.5. Non-Repudiation

This ensures that neither a sender nor a receiver can deny a message that has been transmitted. This also helps in detection and isolation of the compromised node.

3. Attacks on MANET

Since MANET is an infrastructure less network, there are much more security needed as each node in the network my move anywhere. There is also no centralized security mechanism in MANET. Hence this network is highly prone to the effects of malicious nodes. Attacks on MANETs are divided into two categories Active attacks and Passive attacks. In active attacks, the nodes try to affect the proper functionality of the network. This can be made possible through reading and changing the information on the data packets, denial of services, altering the routing path information, hop count etc. However, these attacks can be found easily. The passive attacks do not affect the normal functionality of the network but tries to alter the information inside the data packets. These attacks are harder to find on comparing with active attacks.

The attacks in MANETS are described in detail.

1. Attacks by modifying the metric values: The malicious nodes modify the sequence number; hop count etc., so that the nodes that reach the destination by depending on such metric values will be redirected. These metric values should be lower to find the best path. The malicious nodes change the least small value to the smaller value and thus redirect the normal nodes.

2. Denial of Service: This attack completely redirects the network traffic along the longer route to reach destination which causes unnecessary delay in transmission.

3. Tunneling: In this attack, two or more nodes collide with each other and exchange messages among them along the data routes. Here, these nodes create a short circuit which affects the normal flow of messages that is controlled by the colliding attackers.

4. Spoofing: In this attack, the malicious node can change the IP address or MAC address of any node with the address of any other node. This spoofing can make any node to move out of the network where it belongs to anywhere else.

5. Routing table overflow attacks: In this attack, the malicious node tries to fill the routing table by creating routes to non- existing routes. If the table is full, then no new routes can be entered.

6. Rushing attacks: Generally, in On-Demand routing protocol, only one route request packet is forwarded to find the shortest path to the destination node. The malicious nodes use this mechanism and rush the route request packets more frequently and generate traffic.

4. Secure Routing Mechanisms

Generally, designing the secure routing protocols based on the reactive (on-demand) routing protocols [13], [14] is more efficient. This on-demand routing protocols exhibit better performance with significantly lower overhead than proactive protocols. In this section, the secure routing protocols are discussed.

ARAN– [1] The Authenticated Routing for ad-hoc Routing (ARAN) is a reactive protocol which uses the cryptographic certification for secure routing. In this protocol, the first step requires a trusted certification authority which distributes its public keys to all the nodes in the network. Each node has to

authenticate and to have this public key before connecting into the network. The next step is discovering route for end-to-end authentication for the source to check whether the intended destination is reached. The source begins route instantiation by broadcasting a digitally signed Route Discovery Packet (RDP) which contains the certificate of initiating node, a nonce, a timestamp and the address of the destination node. The nonce and timestamp in the source node prevent replay attacks and detect looping and append signature on the packet. [2] The intermediate nodes verify the signature and if they are authenticated, then removed them and append their own signature in the packets. Thus, each node appends their signature on the packet before forwarding. The source node keeps track of these routes to find weather the route is active or not. The source node receives an error message if the message is received by any inactive node.

SAR– [10] Security Aware Ad-hoc Routing (SAR) influences the discovery of secures routes in a mobile ad hoc environment. It uses security metrics for routing and these security metrics are embedded into the route request packets and are forwarded towards the destination. The node which receives the packet has the key to decrypt the data. If the node finds the path with security metrics, then it sends the route reply to the source node and then forwards the packet towards the destination through the shortest path. It provides the customizable security for the routing protocol message flow. This SAR restricts the scope of flooding for routes.

SEAD – [4] Secure Efficient Ad-hoc Distance Vector Routing (SEAD) is a proactive routing protocol which is designed based on DSDV protocol. This protocol has been designed to work against the modification attacks. This protocol checks the authenticity of data packets by using the hash chain method where the hash key value is used for transmitting the routing update. When a node receives the routing update, it verifies the authentication of each entry of the message. The SEAD uses the clock synchronization between the nodes and provide shared secret key between pair of nodes in order to avoid loops.

ARIADNE–[5] This is an on-demand secure ad-hoc routing protocol with symmetric cryptography based on DSR. For authentication, this protocol uses shared key between the nodes. In this protocol, if a source node wants to transmit a packet with the other node, then it sends a route request (RREQ) to the other nodes which contains the source address, the destination address, an identifier for identifying the route, a TESLA time interval which denotes the expected arrival time of the packet, and a hash chain. When an intermediate node receives the RREQ, it checks for the TESLA time. The hash chain is used to check the authentication. If the data is valid, then it removes the signature of the previous node and appends its own signature and also replaces the old hash chain with the new one and appends a MAC. This MAC value is verified for each hop of the packet by computing the received and computed hash of MAC.

SAODV – [11] Secure Ad-hoc On-demand Distance Vector Routing protocol (SAODV) is designed based on AODV protocol and makes use of asymmetric cryptography and hash chaining. When a node wants to transmit, then it digitally sends the RREQ packet to the next node and the intermediate node verifies the signature and appends its signature and forwards further. The header hash chains in SAODV are used to authenticate the hop count. When a node wants to send a RREQ or RREP it generates a random number called as seed and it selects a maximum hop count which should be set to the TTL value in the header. Whenever an intermediate node receives a RREQ or RREP it verifies the hop count by hashing Max Hop Count- Hop Count times the hash field and check whether the resultant value is same as Top Hash value. The data packet will be dropped by the node if both the values are different from each other. For the data dropped, an error message is created and is sent to the source.

CORE – [7] This CORE protocol is based on repudiation mechanism in which it works for the creation of collaboration between the nodes. This protocol uses the watch dog mechanism and reputation system. It maintains the reputation table in which the past actions of nodes are collected and the watchdog mechanism calculates the functions and stores them in the table. If a node wants to transmit a packet to the neighbour node, then it checks its past actions in the table and decides whether to forward or not. If an intermediate node refuses to forward the packet, then the CORE protocol will reduce the repudiation. This may also lead to the elimination if that intermediate node from the network.

CONFIDANT – [6] The Cooperation of Nodes: Fairness in Dynamic Adhoc Networks protocol is used to find the malicious nodes in the network. This protocols contain some components: the monitor which looks for any misbehaving activity in the network, the trust manager which sends alarm messages to warn others about the malicious nodes, the reputation system which checks the blacklist of any node to find if any anomalous behavior exists before forwarding the packets and the path manger which deletes the path if it contains malicious nodes.

SLSP– The Secure Link State Routing Protocol (SLSP) has been designed to secure the discovery and the distribution of link state information. For security purpose protocol uses the security purpose. The nodes that are involving in transmission contain IP address of their interfaces. This SLSP protocol distributes the public key by itself to the nodes that are within its vicinity. It does not use any central server for this public key distribution. The nodes find their neighbor nodes by periodically distributing the link state information of the node using Neighbor Lookup Protocol (NLP). This protocol floods control packets at very high rates to limit the effectiveness of the attack.

GAME THEORY- [8] The game theory is a tool which analyses the outcome of complex interactions between rational and self-interested entities who always try to reach the best outcome. This Game theory provides techniques to prevent collaboration among nodes. [9] The game theory uses Dynamic Bayesian Game which is used to find malicious activities and behaviors. This game allows the players to have their own private information. The private information includes energy levels of each node. Each node chooses the actions according to their beliefs and private

information during the game. There are two types of players in the game: senders and receivers. The sender's private information is its own type. The receiver does not have any private information. The sender chooses the message according to its type. The receiver receives the message but does not know the type of the receiver.

There are two types of strategies in Dynamic Bayesian Game. They are pure and mixed. In pure strategy, the player cannot change its type once chosen. In mixed strategy, the player can change its type according to the probability distribution. The node's type can be obtained by the belief evaluation calculation. The type of the node is found using the reputation system. It updates the beliefs about the neighbours using the Baye's rule. Then the optimal response is taken against the particular node. In Game theory, the malicious nodes are found and are not used for the transmission. The messages are transferred from source to destination only through the regular nodes.

Table 1. *Comparing the secure routing protocols.*

Secure Routing Protocol	Routing Strategy	Rushing Attack	Denial of Service Attack	Routing Table Modification Attack	Tunneling
ARAN	On-demand	Yes	No	Yes	No
SAR	On-demand	Yes	No	Yes	No
SEAD	Table-driven	Yes	Yes	Yes	Yes
ARIADNE	On-demand	Yes	Yes	Yes	No
SAODV	On-demand	Yes	No	Yes	No
CORE	Table-driven	No	Yes	No	No
CONFIDANT	On-demand	Yes	No	No	Yes
SLSP	Table-driven	Yes	Yes	Yes	No
GAME THEORY	On-demand	No	Yes	Yes	Yes

Table 1 represents the comparison between several secure routing protocols. The attack forms such as rushing attack, denial of service attack, the routing table modification attack and the tunneling attacks are measured for each protocol. To overcome the tunneling effect, several additional techniques are to be implemented. Thus each technique either table driven or on demand, it somehow works in improving the routing efficiency among the nodes.

5. Conclusion

In this paper, several secure routing protocols have been analyzed and also the security threats and the strategies of the nodes are also analyzed. These protocols are compared and the factors have been tabularized. From the analysis, it has been found that no technique can provide security to all the attacks that can affect the networks. Thus no protocol attains all the security goals. Thus more involvement is needed in finding a protocol that can satisfy all these security goals.

References

[1] Seema Mehla et. al. (2010) "Analyzing security of Authenticated Routing Protocol (ARAN), International Journal on Computer Science and Engineering Vol. 02, No. 03, 664-668.

[2] Chuanqi Gong, Sheng Wu and Yanmin Jing (2012) "ARAN protocol analysis and improvement", International conference on System Science, Engineering Design and Manufacturing Informatization, vol. 02, 347-350.

[3] R. Pushpalakshmi and A. Vincent Antony Kumar (2010) "Security aware minimized dominating set based routing in MANET" Second International conference on Computing, Communication and Networking Technologies, 1-5.

[4] Yih-Chun Hu, David B. Johnson, Adrian Perrig (2003)" SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks" ELSEVIER, PA 15213.

[5] Yih Chun Hu, Adrian Perrig and David B. Johnson "Ariadne: A Secure On-Demand Routing Protocol for springer 2005Ad Hoc Networks".

[6] S. Buchegger and J. Y. L. Boudec (2002), "Performance analysis of the CONFIDANT Protocol, cooperation of nodes - Fairness in dynamic ad hoc networks," inProc. IEEE/ACMMOBIHOC, June

[7] P. Michiardi and R. Molva (2002), "CORE:Acollab orative reputation mechanism to enforce node cooperation in mobile ad hoc networks," 6th Joint Working Conf. Commun. and Multimedia Security: Advanced Commun. And Multimedia Security, pp. 107–121.

[8] F. Li and J. Wu (2010), "Attack and Flee: Game theory based analysis on interactions among nodes in MANETs," IEEE Trans. Syst., Man Cybern., vol. 40, pp. 612-622.

[9] Manshaei. M. H et al. (2013), "Game theory meets network security and privacy," J. ACM Comput. Surv, vol. 45, no. 3.

[10] S. Yi, P. Naldurg and R. Krvets, "Security Aware Ad hoc Routing for Wireless networks", Proc. 2nd ACM Symp. Mobile Ad Hoc net. and Comp. (Mobihoc'01), Long Beach, CA, Oct. 2001, pp. 299-302.

[11] M. G. Zapata and N. Asokan, "Secure Ad-Hoc On-demand Distance Vector Routing", ACM Mobile Comp. and Commun. Review, vol. 3, no., July 2002, pp. 106-07.

[12] P. Papadimitratos and Z. J. Haas, "Securing the internet routing infrastructure", IEEE Commun. Mag., vol. 10, no. 40, oct 2002, pp. 60-68.

[13] David B. Johnson and David A. Maltz, Dynamic Source Routing in Ad-Hoc Wireless Networks, Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Kluwer Academic Publishers, Chapter 5, 1996, pp. 153-181.

[14] Charles E. Perkins, Elizabeth M. Royer and Samir R. Das, Ad Hoc On Demand Distance Vector (AODV) Routing, IETF Internet Draft draft-ietfmanet-aodv-08. txt, March 2001.