Security Defence Decision in Mobile Ad hoc networks

Manimozhi.V
PG Scholar, Department of Computer Science,
S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, India.
manimozhi40@gmail.com

Nandhakumar.G
Assistant Professor, Department of Computer Science,
S.K.P Engineering College, Thiruvannamalai, Tamil Nadu, India.
sivanesh09@gmail.com

Kumaresan.A
Phd scholar, Computer Science and Engineering, SKP Engineering College,
Thiruvannamalai, Tamil Nadu, India.

Abstract-In MANET decision-making, key-distribution, routing and forwarding packets are usually decentralized and many of them depend on the cooperative participation among all nodes. MANET is particularly susceptible to several attacks ranging from passive eavesdropping to active interfering due to their open medium; this is in contrast to wired networks, where an opposition must gain physical access to the network wires to be able to make such type of attacks. The main contribution in this paper is to increase the efficiency of intrusion detection system in MANET, by decreasing the false-positives. The modules used in proposed system are node generation, clustering of nodes, Route discovery, shortest distance path, attacker detection such as the node is attacker or not. While using Nash Equilibrium in networks to detect multiple attackers present in MANETs. The Nash equilibrium determines various node strategies in clusters of nodes. Simulation results show that the mobile utility, performance, stability of MANET's, the proposed scheme can enable to prevent attackers with fully distributed nature.

Index Terms: **Network security, MANET, Nash Equilibrium, Proactive table, Intrusion detection system.**

I INTRODUCTION

Mobile Ad Hoc Networks has one of the prevalent areas of research in recent years. It is the new emerging technology which makes users to communicate without any physical infrastructure. MANET is sometimes referred to as an infrastructure less network. An ad-hoc network is self –organizing and adaptive device in mobile ad-hoc networks. It operate in highly dynamic, infrastructure-less and potentially hostile environments, with limited bandwidth and energy resources. Even though security has long been an active research in wire-line networks, the unique characteristics of MANETs gives a set of no trifling challenges to security design. A wireless mobile node can function both as a network router for routing packets from the other nodes and as a network host for transmitting and receiving data. Network topology changes dynamically and unpredictability because of nodes mobility. On the other hand, the unique characteristics of MANET allow new challenges to security design due to lack of any central authority and shared wireless medium. Two complementary classes of approaches exist to protect high security MANETs, prevention-based approaches, such as authentication, and detection-based approaches such as intrusion detection. Continuous authentication and intrusion detection can be considered to improve the performance of high security MANETs. Therefore combining continuous user authentication and intrusion detection can be an effective approach to improve the security performance in high security MANETs. Recently, game theoretic approaches have been proposed to improve network security in IDS. Game theory is a tool to solve multiple-player games. It describes a game by specifying the players involved in the game, in order to which the player take actions, knowledge of the previous actions taken by another player. In game theory assumes each player is rational; this means that each player aims to choose the response that brings the greatest benefit. A Game includes the interactions between nodes in any situation. In mean field game theoretic approach denotes the cooperative, if nodes interact cooperatively. Game theory is used to model the interaction between the defender and attacker. It used to determine which access control strategy is the best for access control system. In this paper is based on security defense decision in mobile ad hoc networks with the help of Nash Equilibrium (NE) algorithm, to detect the neighbor node is attacker or not and proactive scheme is used to generate our shortest distance path between the one node and other in networks. Packets are widely transferring through the clustering of nodes in (MANETS) based on the individual host address in router. According to this search to prevent multiple attackers in networks and their packets are securely transferred from one node to other.

II RELATED WORK

In joint topology based MANET's is mainly focus in security for widely deployed wireless applications that the wireless channels are vulnerable to attacks and their bandwidth is a constrained resource. Security has become the main concern and bottleneck for widely deployed wireless applications. In addition, a discrete stochastic approximation approach has been employed in JATC to deal with the imperfect channel knowledge and the dynamically changing topology. .[1],Security in Mobile AD HOC networks is to supplies protected communication between mobile nodes in hostile environment. The Unique characteristics of MANET 's propose a number of non trifling challenges to security design such as peer-to-peer network architecture, stringiest resource constraints and network topology are the challenges make a case for building multi-fence security solutions to achieve broadband connection and network performance. Here the main security problem of protecting the multi-hop network connectivity between mobile nodes in MANET.[2],An Optimal combined Intrusion detection system and authentication in mobile based networks is mainly based on two complementary classes of approaches exist to protect high security in MANET's. Prevention-based approaches include authentication and detection-based approaches, include intrusion detection. A common framework to enable continuous authentication and intrusion detection jointly may result in a more complex system than designing them separately. The system should be carefully designed taking into account of system security requirements and resource constraints [3], The inherently unprotected characteristics of wireless ad hoc networks make them defenseless against in attacks, and it may be too late before any counter action can take effect. If aggressors try hard enough they will eventually succeed in penetrate the system to monitor audit data and initiate a proper response.[4],Networks provide users with a convenient way to access information and a sufficient communication channel to communicate. Unfortunately, networks have many securities issues including: Internet attacks, cyber crimes, flooding Denial of Service (DoS) attacks, illegal data access, data stealth, etc. Network attacks can cause public institutions or private entities to lose money, important data, or their reputations. Game theoretic approaches have been proposed by many researchers to improve network security. On the one hand, the weakness of traditional solutions to network security is their lack of a quantitative decision framework.[5], The malicious node attacks in an effort to waste the resources and disrupt the operation of the network. Attacking leads to a failure of one round of communication between two neighbors. Malicious nodes can conduct a simple dropping packet attack, which is in the same form as the decline strategy of regular nodes. However, malicious nodes get payoff from the attack, while regular nodes receive no gain from the decline. Malicious nodes can also conduct more sophisticated attacks, such as analyzing a received packet without further forwarding or sending out a modified packet. To make the definition of "attack" more general, we use the cost and gain metrics to summarize the characteristic of one type of attack in the game. Different attack mechanisms have different costs and expected gains; however, the game-based analysis framework is equally applicable to these attacks. Here the regular node forms belief, chooses the probability to cooperate with its opponent based on its belief, and follows a rational decision rule to report. The malicious node keeps evaluating the risk of being caught and exploits its flee strategy to avoid punishment.[6]Although some excellent research has been done on addressing the security issues in MANETs using game theoretic approaches, most of the existing work only considered a security game model with two players an attacker and a user. For the problem scenarios with multiple attackers versus multiple defenders, the security game is usually modeled as a two-player game in which the whole of the defenders is treated as one player, as is the whole of attackers. Consequently, each individual node in a MANET should be treated separately in the security game model.[7]

III EXISTING SYSTEM

Game theory has been used extensively in computer and communication networks to model a variety of problems. In the literature, many schemes propose game theoretic solutions for intrusion detection or security provision within the realm of MANETs. Many approach applied game theory and client puzzles to devise a defense against denial of service (DoS) attacks. It used a game theoretic framework to model intrusion detection via sampling in communications networks. Few works propose game theoretic solutions for intrusion detection or security provision within the realm of MANETs. To the best of our knowledge none of them propose a method of calculating the shielding and attacking probability distributions over MANETs nodes by maximizing the utility of the MANET and any malicious coalition at the NE. Authors use a dynamic Bayesian game framework to analyze the situation between regular and malicious nodes in a MANET. The same authors have examined the dynamic interactions between good nodes and adversaries in MANETs as secure routing and packet forwarding games. Authors have used a game theoretic framework to examine secure cooperation stimulation in autonomous MANETs.

IV PROPOSED SCHEME FOR MOBILE AD HOC NETWORKS

The Game theory model is used in non co-operative security games joining a clustering of nodes; each node is protected by the IDS with various MANETS to form malicious coalition. This work constitutes by finding defender and attackers probability disseminations of MANET with their malicious coalition, that maximize the utility of nodes at mixed strategies of NE of a non co-operative security game model. Based on various node strategy to determine the node is probably working or not. To go a step further, this paper proposes a way of the IDS or attacker's effort is calculating with corresponding energy costs of the MANET. NE strategies are more applicable in all equilibrium strategies of the node; they check various attackers are present in clusters of nodes. While using shortest distance path route decision determine, which one is the right path to reach our destination. Finally a packet is securely transmitted from source to destination. Packet size functions, performance, stability of MANET's are increased as shown in this paper. In our best of our knowledge, we use Nash equilibrium for detecting multiple attacks in MANETS. It is established on more reliability of routing information compared with AODV method.

MIXED STRATEGIES IN NASH EQUILIBRIUM

A Nash Equilibrium occurs in network, when each player is pursuing their best possible strategy in the full knowledge of the other player's strategies. Nash equilibrium is reached when nobody has any incentive to change their strategy. Dominated strategies are never used in mixed Nash equilibrium, even if they are dominated by another mixed strategy. For example in the following game strategy M is dominated by the mixed strategy (0.5U+0.5D) and therefore Player 1 can mix between only U and D.

	Player 2	
	L	R
U	3,1	0,2
Player1 M	1,2	1,1
D	0,4	3,1

In other words finding its mixed strategy Nash equilibrium is equivalent to finding the mixed Nash equilibrium of the following game:

	Player 2	
	L	R
Player 1 U	3,1	0,2
D	0,4	3,1

Indeed only the strategies that survive iterated elimination of dominated strategies can be used in mixed Nash equilibrium.

Example: In the following game M is dominated by U for
Player 1 and next m is dominated by l for Player 2:

		Player 2		
		L	M	R
Player1	U	3,2	3,1	1,3
	M	2,1	1,5	0,3
	D	1,3	4,2	2,2

1. NODE GENERATION

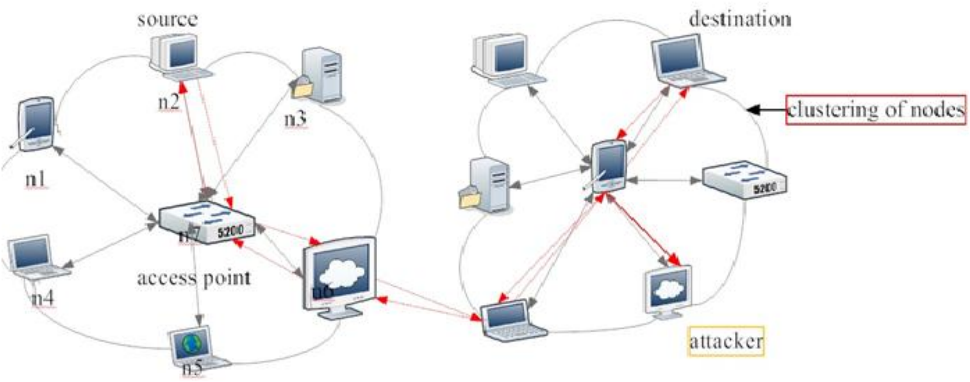
In this model, user can create more nodes for transferring the various sizes of packets in MANETS. In general MANET is free to move individually in any direction and will change its links to the devices frequently. Here mobile device also act as a router for transferring packets from one clustering of nodes to the other. For our assumption, more users are acting as a node to generate various types of nodes. Based on the node generation, various nodes are act as a router to form a clustering of nodes. Users can carry their mobile devices physically gather in public places such as University campus, work place, shopping complexes and airports etc. in this places MANETs can be formed using Ad hoc wireless connections between the devices. In which individual devices can communicate each other. The deployment of wireless nodes where there is no infrastructure or the local infrastructure is not reliable can be difficult. With the existence of such networks an alternative approach to content retrieve by a device would be to first search local MANET for the requested content before downloading it from the CP’s server. The retrieved object provisioning cost of such a proposal can be significantly lower since the download cast to the CSP. It can be avoided when the content is found within the local MANET.

2. CLUSTERING

Clustering can be used for routing efficiency in wireless networks. Unassociated clusters are established to schedule transmissions in a contention-free way. Individual cluster has a cluster head, one or more portals and zero or more regular nodes. Cluster head schedules transmission and allocates resources with its cluster. Gateways connect adjacent clusters. Discover neighbors are establishing link-clustered control structure. The node with minimum node-id is selected to be a cluster head. A node is called a portal, if it lies within the transmission range of two or more clusters. Disseminated gateway is a pair of nodes that inhabit within different clusters, but they are within the transmission range of each other.

3. ROUTE DISCOVERY

Route discovery allows any host to dynamically discover the route to any destination in the ad hoc network. When a node has a data packet to send, it first checks its own routing cache. If it finds a valid route in its own routing cache, it sends out the packet using this route. Otherwise, it initiates a route discovery process by broadcasting a route request packet to all entire neighbor. The route request packet contains the source address, the request id and a route record in which the sequence of hops traversed by the request packet, before reaching the destination is recorded. A node upon getting a route request packet does the following. If a packet does not have the required route in its routing cache, it forwards the packet to its entire neighbor. A node forwards a route request message only if it has not yet seen it earlier, and if it is not the destination. The route request packet initiates a route request packet initiates a route reply upon reception either by the destination node or by an intermediate node that knows a route to the destination. Upon arrival of the route request message at the destination, this information is piggybacked on to the route reply message that contains the path information and is sent to the source node.



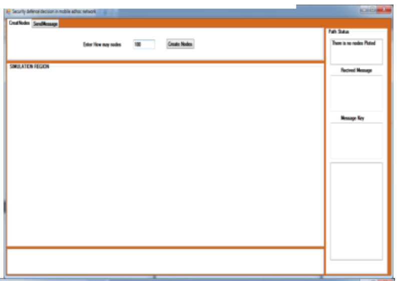
4. SHORTEST PATH

\ Based on clustering of nodes, each cluster has a router with the communication of every access points. Each and every router can generate a shortest distance path between transmitter and receiver. Finally routers can create a pro-active routing table. Pro-active routing table includes host ip address of neighbor nodes, shortest distance path, neighbor node, receiver node address. Pro-active routing table is used to update the shortest path links within the time interval.

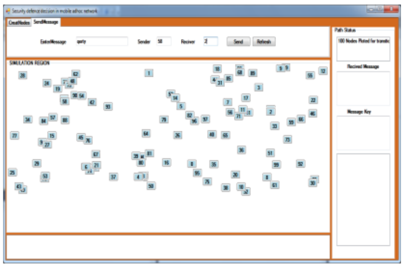
5. ATTACKER DETECTION

A large number of packets are transmitted from transmitter to receiver in wireless mobile ADHOC networks. Multiple attackers are exist in network medium to access a required packets based on the mobility, packet size, various locations. To prevent multiple attackers, we use Nash equilibrium to check each node is act as a router or attacker in network environment. Once the process is completed, the packet is securely transmitted from one node to another.

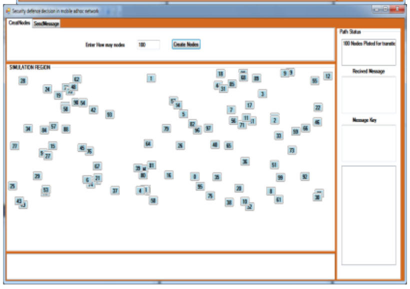
VI RESULTS



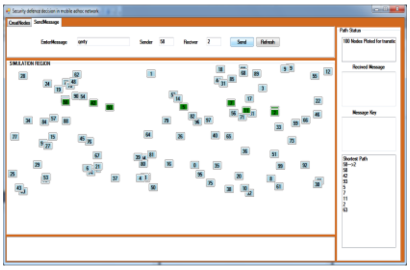
There is no nodes Plotted



100 Nodes Ploted for transtic



100 Nodes Ploted for transtic



100 Nodes Ploted for transtic

Shortest Path
58-->2
58
42
93
5
7
11
2
63

VII CONCLUSION

In this paper, we proposed Nash Equilibrium for security in MANETs to model the interactions among a malicious node and a large number of legitimate MANET nodes. Unlike the existing works on security game modeling, the proposed scheme provides a distributed security defense decisions in MANETS. Both security requirement and system resources were considered in the proposed scheme. This paper prevents a multiple attackers in MANETs using proactive routing protocol with the usage of Nash Equilibrium. The simulation results demonstrated that, with the mobile utility, the legitimate nodes can choose distributed actions intelligently to reduce their energy consumption and security value loss. The average lifetime of the MANET can be improved significantly and the compromising probability can be reduced as well. In our future work, we will extend our proposed scheme to the scenario of multiple attackers and multiple defenders.

REFERENCES

1. Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh Technol.*, vol. 61, no. 6, pp. 2674–2685, July 2012.
2. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 38–47, Feb. 2004.
3. J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2,.pp. 806–815, Feb. 2009.
4. Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in *Proc. 2000 ACM MOBICOM*, pp. 275–283.
5. X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 2013.
6. F. Li, Y. Yang, and J. Wu, "Attack and flee: game-theory-based analysis on interactions among nodes in MANETs," *IEEE Trans. Syst., Man, Cybern. (B)*, vol. 40, pp. 612–622, June 2010.
7. Yanwei Wang, F. Richard Yu, *Senior Member,"* A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks,*" IEEE* Transactions on Wireless Communications, Vol. 13, no. 3, pp. 612-622,March 2014.