ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Puzzle Based Defense Mechanism for Security Enhancements in MANETs

M Sivakumar, V S Sinduja

M.E., Assistant Professor, Paavai College of Engineering, Namakkal, India.

PG Scholar, Paavai College of Engineering, Namakkal, India.

ABSTRACT: The mean field game theory provides a powerful mathematical tool for problems with a large number of players. In the existing system, a novel game theoretic approach with multiple players for security is used in MANETs. The existing scheme can enable an individual node in MANETs to make strategic security defense decisions without centralized administration. In addition, since security defense mechanisms consume precious system resources (e.g., energy), the existing scheme considers not only the security requirement of MANETs but also the system resources. Moreover, each node in the existing scheme only needs to know its own state information and the aggregate effect of the other nodes in the MANET. This paper utilizes game theory to propose a series of optimal puzzle-based defense mechanism for security enhancement in MANETs. In doing so, the solution concept of Nash equilibrium is used in a prescriptive way, where the defender takes his part in the solution as an optimum defense against rational attackers. Proposed scheme is based on the Sequential Probability Ratio Test which is a statistical decision process for tackling the mobile replica detection problem. This study culminates in a strategy for handling distributed attacks from an unknown number of sources.

I. INTRODUCTION

Mobile ad-hoc network (MANET) which is a self-configuring network of mobile routers and associated hosts are connected by wireless links, the union of which form a random topology. MANET may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make MANET suitable for emergency situations like natural or human induced disasters, military conflicts. To address the security issues in MANETs using game theoretic approaches, most of the existing work only considered a security game model with two players in the security game model: an attacker and a defender. 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. While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available. Consequently, each individual node in a MANET should be treated separately in the security game model. The active entities, know the past events, and hence, the histories at any state, the game among them is of perfect information in which a player can condition his action choice at later states on the actions taken by the other players at previous states.

II. LITERATURE SURVEY

Helen Tang, Minyi Huang, Richard Yu, Yanwei Wang(2014) together proposed a dynamic mean field game theoretic approach to enable an individual node in MANETs to make strategic security defence decisions without centralized administration. Most of the existing work only considered a security game model with two players in the security game model: an attacker and a defender. 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. Since security defence mechanisms in a wireless mobile node consume precious system resources (e.g., energy), the proposed scheme considers not only the security requirement of MANETs but also the system resources. In the proposed mean field game theoretic approach, each node only needs to know its own state information and the aggregate effect of the other nodes in the MANET. The proposed scheme is a fully distributed scheme. System contains

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

an N-node MANET and an attacker. Then the security problem of this system is formulated as an N + 1 mean field game.

H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang (2004) together focus on the fundamental security problem of protecting the multi-hop network connectivity between mobile nodes in a MANET. This identify the security issues related to this problem, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and network- layer operations of delivering packets over the multi-hop wireless channel. The complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction.

F. R. Yu, H. Tang, S. Bu, D. Zheng (2013) Proposed is a game-theoretic approach to quantitatively analyze the attack strategies of the attacker so as to make a rational decision on relay selection and the authentication parameter adaptation to reach a trade-off between security and QoS in CO-MANETs. Cooperative communication has been considered as a promising technique to improve communication quality of service (QoS) in wireless networks, including mobile ad hoc networks (MANETs). Due to their unorganized and decentralized infrastructure, cooperative MANETs (CO-MANETs) are vulnerable to attacks initiated on relays. Although encryption and authentication protocols may prevent compromised data transmission when a selected relay is attacked, their cost is high.

Q. Guan, F. R. Yu, S. Jiang, V. Leung (2012) jointly considers authentication and topology control. Specifically, analyzes the effective throughput with upper layer authentication schemes and physical-layer schemes related to channel conditions and relay selections for CCs. A joint authentication and topology control (JATC) scheme is proposed to improve the throughput. JATC is formulated as a discrete stochastic optimization problem.

J. Liu, F. R. Yu, C. Lung, H. Tang (2009) together proposed a framework combining intrusion detection and continuous authentication in MANETs. In this framework, multimodal biometrics is used for continuous authentication, and intrusion detection is modeled as sensors to detect system security state. The whole system is formulated as a partially observed Markov decision process considering both system security requirements and resource constraints. Then it uses dynamic programming-based hidden Markov model scheduling algorithms.

S. Bu, F. R. Lu, X. P. Liu, H. Tang (2011) jointly obtained the optimal scheme of combining continuous user authentication and IDSs in a distributed manner, the problem is formulated as a partially observable Markov decision process (POMDP) multi-armed bandit problem. Considering these two approaches jointly is effective in optimal security design taking into account system security requirements and resource constraints in MANETs.

X. Liang, Y. Xiao (2013) together introduced Game theoretic approaches as a useful tool to handle those tricky network attacks. Reviewed the existing game-theory based solutions for network security problems, classified their application scenarios under two categories, attack-defense analysis and security measurement. Presents a brief view of the game models in those solutions and summarize them into two categories, cooperative game models and non-cooperative game models with the latter category consisting of subcategories.

A. Patcha, J. M. Park (2006) present a game-theoretic model to analyze intrusion detection in mobile ad hoc networks. This uses game theory to model the interactions between the nodes of an ad hoc network. Viewing the interaction between an attacker and an individual node as a two player non-cooperative game, and construct models for such a game.

F. Li, Y. Yang, J. Wu (2010) proposed a game theoretic framework to analyze the strategy profiles for regular and malicious nodes. The situation is modelled as a dynamic Bayesian signaling game and it analyze and present the underlining connection between nodes' best combination of actions and the cost and gain of the individual strategy. Regular nodes consistently update their beliefs based on the opponents' behaviour, while malicious nodes evaluate their risk of being caught to decide when to flee. Some possible countermeasures for regular nodes that can impact malicious nodes' decisions are presented as well.

III. PROPOSED SYSTEM

The Proposed system utilizes a dynamic mean field game theoretic approach to enable an individual node in MANETs to make strategic security defense decisions without centralized administration. Since security defense mechanisms in a wireless mobile node consume precious system resources (e.g., energy), the proposed scheme considers not only the security requirement of MANETs but also the system resources. In the proposed mean field game theoretic approach, each node only needs to know its own state information and the aggregate effect of the other

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

nodes in the MANET. Therefore, the proposed scheme is a fully distributed scheme.The Proposed System utilizes game theory to propose puzzle-based defense mechanism for Security enhancements in MANETs. The interactions between an attacker and a defender can be modeled as an infinitely repeated game of discounted payoffs. The solution concepts of this type of games are deployed to find the solutions, i.e., the best strategy a rational defender can adopt in the face of a rational attacker. In this way, the optimal puzzle-based defense strategies are developed. The mechanism is such that regardless of what happens in the history, using closed-loop solution concepts, the defender defeats both single-source attack and distributed attacks. The system works well even when the size of the size of the attack coalition is unknown. Fortunately, mobility provides us with a clue to help resolve the mobile replica detection problem. Specifically, a benign mobile sensor node should never move faster than the system-configured maximum speed, Vmax. As a result, a benign mobile sensor node's measured speed will appear to be at most Vmax as long as the employed solution is a speed measurement system with a low rate of error.

IV. SEQUENTIAL PROBABILITY RATIO TEST

Fortunately, mobility provides us with a clue to help resolve the mobile replica detection problem. Specifically, a benign mobile sensor node should never move faster than the system-configured maximum speed, Vmax. As a result, a benign mobile sensor node's measured speed will appear to be at most Vmax as long as the employed solution is a speed measurement system with a low rate of error. Replica nodes will appear to move much faster than benign nodes and thus their measured speeds will likely be over Vmax because they need to be at two (or more) different places at once. Accordingly, if the mobile node's measured speed exceeds Vmax, it is then highly likely that at least two nodes with the same identity are present in the network. Proposed is a mobile replica detection scheme by leveraging this intuition. Our scheme is based on the Sequential Probability Ratio Test which is a statistical decision process.

The SPRT can be thought of as one-dimensional random walk with the lower and upper limits. Before the random walk starts, null and alternate hypotheses are defined in such a way that the null hypothesis is associated with the lower limit while the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation. If the walk reaches (or exceeds) the lower or upper limit, it terminates and the null or alternate hypothesis is selected, respectively. SPRT is well suited for tackling the mobile replica detection problem since one can construct a random walk with two limits in such a way that each walk is determined by the observed speed of a mobile node. The lower and upper limits can be configured to be associated with speeds less than and in excess of Vmax, respectively. Method of applying the SPRT to the mobile replica detection problem is as follows: Each time a mobile sensor node moves to a new location, each of its neighbours asks for a signed claim containing its location and time information and decides probabilistically whether to forward the received claim to the base station. The base station computes the speed from every two consecutive claims of a mobile node and performs the SPRT by considering speed as an observed sample. Each time the mobile node's speed exceeds (respectively, remains below) Vmax, it will expedite the random walk to hit or cross the upper (respectively, lower) limit and thus lead to the base station accepting the alternate (respectively, null) hypothesis that the mobile node has been (respectively, not been) replicated. Once the base station decides that a mobile node has been replicated, it revokes the replica nodes from the network

V. SYSTEM ARCHITECTURE

System Architecture diagram depicts the working model of the proposed solution. The proposed method utilizes game theory to define puzzle-based defenses for security in MANETs. The interactions between an attacker who launches an attack and a defender who counters the attack using a puzzle-based defense can be modeled as an infinitely repeated game of discounted payoffs.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

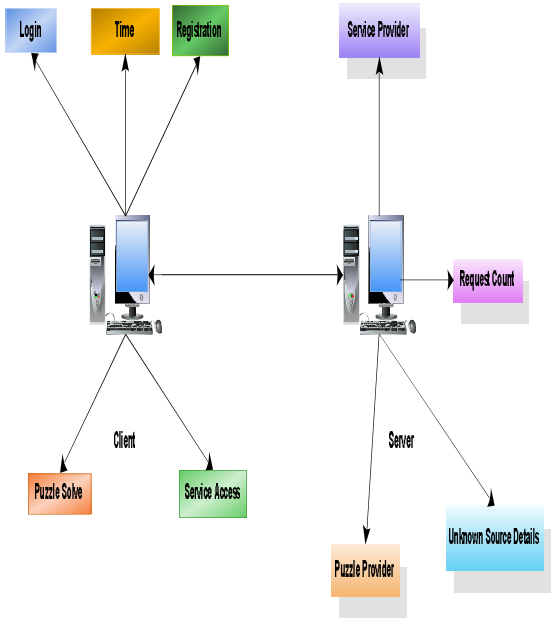

Fig 1. System Architecture

VI. CONCLUSION

The proposed method utilizes game theory to define puzzle-based defenses against flooding attacks. The interactions between an attacker who launches a flooding attack and a defender who counters the attack using a puzzle-based defense can be modeled as an infinitely repeated game of discounted payoffs. Then, the solution concepts of this type of games are used to find the solutions, i.e., the best strategy a rational defender can adopt in the face of a rational attacker. The solution supports the open-loop solution concept in which the defender chooses his actions regardless of what happened in the game history. This mechanism is applicable in defeating the single-source and distributed attacks and also supports the higher payoffs being feasible in the game. An integrated with reactive defenses to achieve synergetic effects. In this way, the optimal puzzle-based defense strategies are developed.

REFERENCES

1. Bu. S, Tang. H, Yu. F. R, Zheng. D (2013), "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks", EURASIP J. Wireless Communication Networks, vol. 2013, no. 1, pp. 188–190.
2. Bu. S, Liu. X. P, Tang. H, Yu. F. R (2011), "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks", IEEE Transactions. Wireless Communication, vol. 10, no. 9, pp. 3064–3073.
3. Guan. Q, Jiang. S, Leung. V, Yu. F. R (2012), "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications", IEEE Transactions Veh. Technol., vol. 61, no. 6, pp. 2674–2685.
4. Helen Tang, Minyi Huang, Richard Yu, Yanwei Wang (2014), "A Mean Field Game Theoretic Approach For Security Enhancements in Mobile Ad hoc Networks", IEEE Trans. Wireless Communication, vol. 13.
5. Lee. W, Zhang. Y (2000), "Intrusion detection in wireless ad hoc networks", in Proc. 2000 ACM MOBICOM, pp. 275–283.
6. Li. F, Yang. Y, Wu. J (2010), "Attack and flee: game-theory-based analysis on interactions among nodes in MANETs", IEEE Transactions. System, Man, Cybern. (B), vol. 40, pp. 612–622.
7. Liang. X, Xiao. Y (2013), "Game theory for network security", IEEE Communication Surveys Tuts., vol. 15, no. 1, pp. 472–486.
8. Liu. J, Lung. C, Tang. H, Yu. F. R (2009), "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks", IEEE Transactions Wireless Communication, vol. 8, no. 2,pp. 806–815.
9. Lu. S, Luo. H, Yang. H, Ye. F, Zhang. L (2004), "Security in mobile ad hoc networks: challenges and solutions", IEEE Trans. Wireless Communication, vol. 11, pp. 38–47.
10. Omic. J, Orda. A,Van Mieghem. P (2009), "Protecting against network infections:a game theoretic perspective", in Proc. 2009 IEEE INFOCOM,pp. 1485–1493.
11. Patcha. A, Park. J.M (2006), "A game theoretic formulation for intrusion detection in mobile ad hoc networks", Int'l J. Netw. Security, vol. 2,no. 2, pp. 131–137.
12. William Stallings, Cryptography and Network Security: Principles and Practice, 2013.
13. Menezes Bernard, Network Security and Cryptography, 2011.
14. Jonathan Loo, Jaime Lloret Mauri, Jesus Hamilton Ortiz, Mobile Adhoc Networks: Current Status And Future Works, 2011