World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 4.326

A NOVEL TECHNIQUE FOR EFFICIENT USAGE OF INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORKS

Anushree Ashok Wasu* and Prof. P. D. Thakare.

J. C. O. E. T. Yavatmal.

Article Received on 01/12/2017 **Article Revised on 22/12/2017** **Article Accepted on 12/01/2018**

***Corresponding Author**
Anushree Ashok Wasu
J. C. O. E. T. Yavatmal.

ABSTRACT

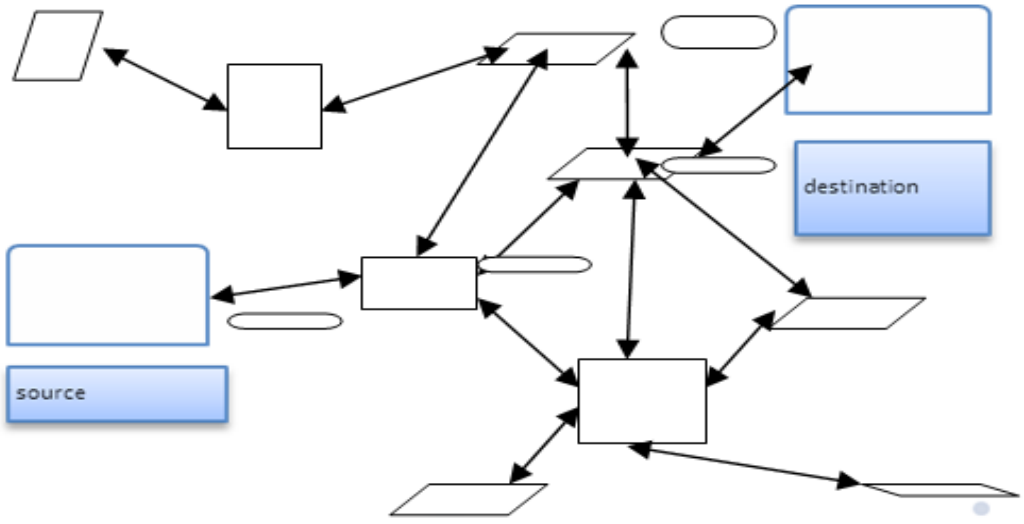
Mobile Ad hoc Networks (MANET) are selfconfiguring, infrastructureless, dynamic wireless networks in which the nodes are resource constrained. Intrusion Detection Systems (IDS) are used in MANETs to monitor activities so as to detect any intrusion in the otherwise vulnerable network in this paper; we present efficient Schemes for analyzing and optimizing the time duration for which the intrusion detection systems need to remain active in a mobile ad hoc network. A probabilistic model is proposed that makes use of cooperation between IDSs among neighborhood nodes to reduce their individual active time. Usually, AN ID has to run all the time on every node to oversee the network behavior. This can turn out to be a costly overhead for a battery-powered mobile device in terms of power and computational resources. Hence, in this work our aim is to reduce the duration of active time of the IDSs without compromising on their effectiveness. To validate our proposed approach, we model the interactions between IDSs as a multi-player cooperative game in which the players have partially cooperative and partially conflicting goals. We theoretically analyze this game and support it with simulation results.

KEYWORDS: A *mobile ad hoc network* (MANET) is a self-organized collection of mobile nodes.

INTRODUCTION

A *mobile ad hoc network* (MANET) is a self-organized collection of mobile nodes which communicate with each other without the help of any fixed infrastructure or central

coordinator. . MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for "Mobile Ad Hoc Network" A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. A node can be any mobile device with the ability to communicate with other devices. In a MANET, a node behaves as a host as well as a router. A node intending to communicate with another node that is not within its communication range, takes help of intermediate nodes to relay its message. The topology of the network dynamically changes over time as nodes move about, some new nodes join the network or few other nodes disengage themselves from the network. MANETs have distinct advantages over traditional networks in that they can easily be set up and dismantled, apart from providing flexibility as the nodes are not tethered. Besides being operable as a stand-alone network, ad hoc networks can also be attached to the Internet or other networks, there by extending connectivity and coverage more importantly to areas where there are no fixed infrastructures. Present and future MANET applications cover a variety of areas. One important application scenario is vehicular ad hoc network (VANET). VANET is a self-configuring network of moving vehicles (i.e., a vehicle is a node) although the movement pattern of nodes are restricted by the road course, traffic regulations, etc. VANET is a promising technology that has tremendous potential to improve vehicle and road safety, traffic efficiency and convenience.[1,2]



Structure of MANET

1.1 How MANET works?

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion and other factors.

Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANETs are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET specifications and management features. Using mature components from previous work on experimental reactive and proactive protocols, the WG will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol (RMP)
- Proactive MANET Protocol (PMP)

If significant commonality between RMRP and PMRP protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be supported. Routing security requirements and issues will also be addressed.

The MANET WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes. The primary purpose of this mechanism is a simplified best effort multicast forwarding function. The use of this protocol is intended to be applied ONLY within MANET routing areas and the WG effort will be limited to routing layer design issues.

The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG and IRTF work that is addressing research topics related to MANET environments.

2. Characteristics of MANET's

- In MANET, each node acts as both host and router. That is it is autonomous in behavior.
- Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.

- The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are characterized with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

2.1 Infrastructure-based Networks

- ❖ Fixed backbone
- ❖ Nodes communicate with access point
- ❖ Suitable for areas where APs are provided

2.2 Infrastructure-less Networks

- ❖ Without any backbone and access point
- ❖ Every station is simultaneously router

2.3 Nodes

- ❖ limited resources
- ❖ dynamic topology
- ❖ Address assignment

2.4 Wireless channels

- ❖ relatively high error rate
- ❖ high variability in the quality
- ❖ low bandwidth
- ❖ broadcast nature
- ❖ security aspect

2.5 Advantages of MANET's

- Wireless communication

- Mobility
- Do not need infrastructure
- but can use it, if available
- small, light equipment

2.6 Disadvantages of MANET's

- Wireless Communication reliability, bandwidth
- Mobility partitioning
- Cannot count on infrastructure
- Small, Light equipment Limited resources(memory, battery power)

3. Types of MANET

There are different types of MANETs including:

- In VANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
- Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipments.
- Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

4. Proposed Work

Cooperative game theory can be used to model situations in which players coordinate their strategies and share the payoffs between them. The output of the game (individual payoffs that players receive) must be in equilibrium so that no player has incentive to break away from the coalition.[33,35] The game settings in all the earlier game-theoretic work on IDS involves two sets of opposing players, the nodes/IDSs and the attacker/defaulters. In our work, we have set a game that involves players (IDSs sitting in neighboring nodes) cooperating to achieve a common goal (i.e., to monitor a single node). To the best of our knowledge, we have not come across any work on cooperating IDSs (to get a security versus energy tradeoff) that models such a situation using game theory. We have presented such a cooperative multi-player game to model the interactions between the IDSs in a neighborhood and used it to validate our proposed probabilistic scheme. The contributions of this paper are summarized as follows:

1. We present a novel technique, based on a probabilistic model, to optimize the active time duration of intrusion detection systems (IDSs) in a MANET. The scheme reduces the IDSs' active time as much as possible without compromising on its effectiveness.
2. To validate our proposed approach, we also present a multi-player cooperative game that analyzes the effects of individual intrusion detection systems with reduced activity on the network.
3. Through simulation we show that a considerable saving in energy and computational cost is achieved using our proposed technique of optimizing the active time of the IDSs while maintaining the performance of the IDS.
4. The proposed scheme uses local information, thus making it distributed and scalable. Moreover, it works on both static and mobile networks.

CONCLUSION

In this project we have proposed an efficient way of usingintrusion detection systems (IDSs) that sits on every node of a mobile ad hoc network (MANET). We first present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem.We then described a cooperative game model to represent the interactions betweenthe IDSs in a neighbourhood of nodes. The game is defined in such a way that the primary goal of the IDSs is to monitor the nodes in its neighbourhood at a desired security level so as to detect any anamolousbehaviour, whereas, the secondary goal of the IDSs is to conserve as much energy as possible. To achieve these goals, each of the nodes has to participate cooperatively in monitoring its neighbour nodes with a minimum probability. We then develop a distributed scheme to determine the ideal probability with which each node has to remain active (or switched on) so that all the nodes of the network are monitored with a desired security level. The evaluation of the proposed scheme is done by comparing the performances of the IDSs under two scenarios: (a) keeping IDSs running throughout the simulation time and (b) using our proposed scheme to reduce the IDS's active time at each node in the network. From the simulation results we observe that the effectiveness of the IDSs in the network is not compromised while using the proposed scheme, rather, there is considerable reduction of energy consumption in each of the nodes that increases the network lifetime significantly. Here we have assumed a homogeneous network in a way that all the nodes have the same capacities in terms of their computational andenergy resources. In future we wish to extend our model toaccommodate a heterogeneous network.

REFERENCES

1. S. Zeadally, R. Hunt, Y-S. Chen, A. Irwin and A. Hassan, "Vehicular adhoc networks (VANETS): status, results, and challenges," Telecommunication Systems, 2012; 50(4): 217-241.
2. S. K. Bhoi and P. M. Khilar, "Vehicular communication: a survey", IET Networks, 2014; 3(3): 204 - 217.
3. S. Marti, T. J. Giuli, K. La and M. Baker, "Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment," Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2000; 255- 265.
4. C. Manikopoulos and L. Ling, "Architecture of the Mobile Ad-hoc Network Security (MANS) System," Proc. IEEE International Conference on Systems, Man and Cybernetics, 2003; 4: 3122- 3127.
5. K. Nadkarni and A. Mishra, "Intrusion Detection in MANETs – The Second Wall of Defense," Proc. IEEE Industrial Electronics Society Conference, 2003; 1235-1239.
6. Roanoke, Virginia, USA, 2003; 2-6.
7. A. Partwardan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad-hoc Networks," Proc. 3rd IEEE International Conference on Pervasive Computing and Communications, Hawaii Island, Hawaii, March, 2005; 8-12.
8. N. Marchang and R. Datta, "Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks," IET Information Security, 2012; 6(4): 77-83.
9. N. Marchang and R. Datta, "Collaborative Techniques for Intrusion Detection in Mobile Ad-hoc Networks," Elsevier Ad Hoc Networks, 2008; 6(4): 508-523.
10. D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang, "Edge Self-Monitoring for Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, 2011; 22(3): 514-527.
11. I. Khalil, S. Bagchi and N. B. Shroff, "SLAM: Sleep-Wake AwareLocal Monitoring in Sensor Networks," Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007; 565-574.
12. T. Hoang Hai and E-N. Huh, "Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks," Proc. FutureGeneration Communication and Networking (FGCN 2007), 2007; 1: 350-355.
13. S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu, "On modeling energysecurity trade-offs for distributed monitoring in wireless ad hoc networks," Proc. Military Communications Conference, MILCOM 2008. IEEE, 2008; 1-7: 16-19.

14. R. G. Clegg, S. Clayman, G. Pavlou, L. Mamatas and A. Galis, "On the Selection of Management/Monitoring Nodes in Highly Dynamic Networks," IEEE Transactions on Computers, 2013; 62(6): 1207-1220.
15. R. Zheng, T. Le and Z. Han, "Approximate Online Learning Algorithms for Optimal Monitoring in Multi-Channel Wireless Networks," IEEE Transactions on Wireless Communications, 2014; 13(2): 1023-1033.
16. N. Tsikoudis, A. Papadogiannakis and E. P. Markatos, "LEoNIDS: a Low-latency and Energy-efficient Network-level Intrusion Detection System," IEEE Transactions on Emerging Topics in Computing, 2014; 99.
17. R. Muradore and D. Quaglia, "Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security," IEEE Transactions on Industrial Informatics, 2015; 11(3): 830-840.
18. S. Shen, "A game-theoretic approach for optimizing intrusion detection strategy in WSNs," Proc. 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011; 4510-4513: 8-10.
19. A. Afgah and S. K. Das and K. Basu, "A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks," Proc. VTC, 2004.
20. T. Alpcan and T. Basar, "A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection," Proc. 43rd IEEE Conference on Decision and Control, 2004.
21. Y. Liu, H. Man and C. Comaniciu, "A Game Theoretic Approach to Efficient Mixed Strategies for Intrusion Detection," Proc. IEEE International Conference on Communications, 2006.
22. Y. Liu, C. Comaniciu and H. Man, "Modeling Misbehavior in Ad Hoc Networks: A Game Theoretic Approach for Intrusion Detection," International Journal of Security and Networks, 2006; 1: 3-4.
23. L. Chen and Jean Leneutre, "A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks," IEEE Transactions of Information Forensics and Security, 2009; 4(2).
24. A. Patcha and J. Park, "A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks," International Journal of Network Security, vol. 2, no. 2, pp. 146-152, March 2006.

25. N. Zhang, W. Yu, X. Fu and S. K. Das, "Maintaining Defender's Reputation in Anomaly Detection Against Insider Attacks," IEEE Transactions on Systems, Man, and Cybernetics-Part B:Cybernetics, 2010 40(3): 597-611.
26. P. Michiardi and R. Molva, "A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad Hoc Networks," Proc. Wi Opt Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2003.
27. A. Afgah, S. K. Das and K. Basu, "A Game Theory based Approach for Security in Wireless Sensor Networks", Proc. International Performance Computing and Communications Conference (IPCCC), 2004.
28. S-K. Ng and W. K. G. Seah, "Game-Theoretic Approach for Improving Cooperation in Wireless Multihop Networks," IEEE Transactions on Systems, Man, and Cybernetics-Part B:Cybernetics, 2010; 40(3): 559-574.
29. M. F´eleyh´azi, J-P. Hubaux and L. Butty´an, "Nash Equilibria of packet Forwarding Strategies in Wireless Ad Hoc Networks," IEEE ransactions on Mobile Computing, 2006; 5(5): 463-476.
30. F. Li, Y. Yang and J. Wu, "Attack and Flee: Game-Theoretic-Based Analysis on Interactions Among Nodes in MANETs," IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics, 2010; 40(3): 512-622.
31. D. Brauckhoff, K. Salamatian and Martin May, "A Signal Processing View on Packet Sampling and Anomaly Detection," Proc. INFOCOM, 2010.
32. G. Owen, *Game Theory*, 3rd Edition, Academic Press, 2001.
33. C. E. Perkins and E.M. Royer, "Ad-hoc On-Demand Vector Routing," Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, 1999. 90-100
34. J. Lemaire, "Cooperative Game Theory and its Insurance Applications," Astin Bulletin, 21(1).
35. B. Peleg and P. Sudholter, "Introduction to the Theory of Cooperative Games," Second Edition, Springer, 2007.
36. E-Y. Gura and M. B. Maschler, "Insights into Game Theory," Cambridge University Press, 2008.
37. "The Network Simulator - ns2," www.isi.edu/nsnam/ns/.
38. L. M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, 2001; 6: 239-249.

39. L. M. Feeney, "Investigating the Energy Consumption of an IEEE 802.11 Network Interface," Technical Report, ISRN: SICS-T- 99/11-SE, ISSN 1100-3154, Swedish Institute of Computer Science, www.sics.se/ lmfeeney.
40. D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing (T. Imielinski and H. Korth, editors), Kluwer Academic Publishers, 1996; 153-181.
41. I. Khalil, S. Bagchi and N. B. Shroff, "Lite Worp: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," Proc. IEEE International Conference on Dependable Systems and Networks (DSN'05), 2005; 612-621.