RESEARCH ARTICLE OPEN ACCESS

A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile AD HOC Network

P.kavimozh[1] , K.Kasthuri[2] , S.Selvakumari[3]

[1,2]PG student Dept, of Cs & It Dhanalakshmi Srinivasan College of Arts & Science for Women , Perambalur, Tamilnadu ,India

[3]Assistant professor,dept of. Cs & It Dhanalakshmi Srinivasan College of Art & Science for Women, Perambalur ,Tamilnadu,India

Abstract:

Mobile Ad hoc Networks (MANET) are self configuring, 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. 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 IDS 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.

INTRODUCTION

In a MANET, a node behaves as a host as well as a *routerA* mobile ad hoc network (MANET) is collection of mobile nodes which communicate with each other without the help of any fixed infrastructure or central coordinatorIntrusion and has been classified into two broad categoriesbased on the techniques adopted, viz.,

(a) Signature-based intrusion detection . (b) Anomaly-based intrusion detection.

In signature-based detection, knowledge about the signatures of attacks is incorporated in the detection system.In anomaly-based detection, the IDS does not attempt to find a signature match but searches for anomalous events or behaviour.On the other hand, network-based IDSs collect and analyze data from network traffic. In our work, we concentrate on network-based anomaly detection.

EXITING SYSTEM

The existing work focus on reducing the number of monitor nodes that monitor communication link.The protocol SLAM makes use of special nodes called guard nodes for local monitoring in sensor networks.The main aim of the protocol is to reduce the time a guard node remains awake for the purpose of monitoring malicious activities.when a large number of communication links are in use, almost all

the guard nodes in SLAM might be awake, which is also a downside of the protocol..

DISADVANTAGES

- May not hold for some other kind of malicious neighbour.
- Nodes may replay false replay.
- Node checking will not work in the extreme case.

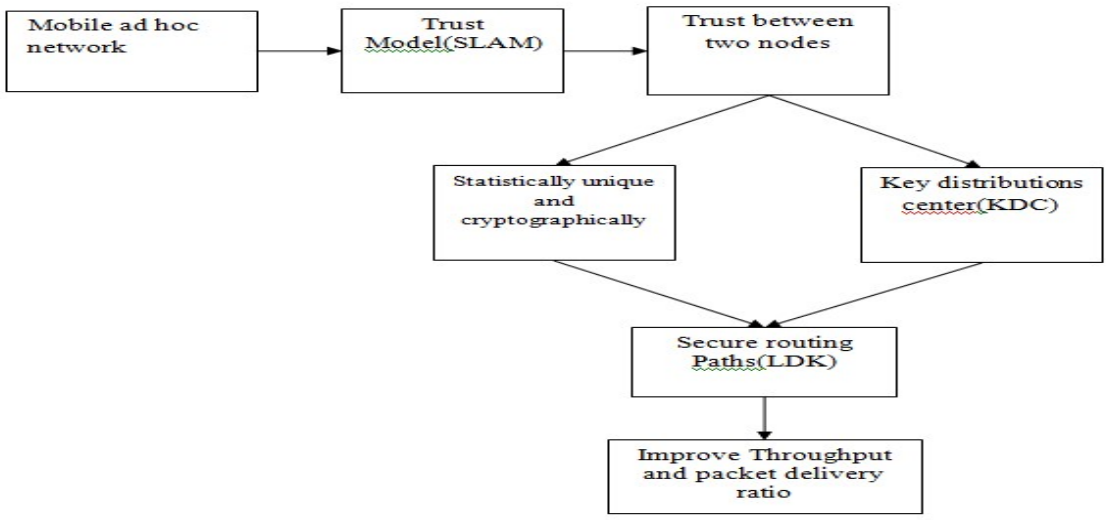
PROPOSED SYSTEM

Additionally, the effect of using Algorithm LDK is that a node (IDS component) samples the behavior of a neighbour node instead of monitoring it all the time.It has been found that the sampling rate of an IDS affects its performance.In the case of a cooperative IDS, these components cooperate and share their observations to finally detect any anamolous behaviour.

ADVANTAGES

- We use the Algorithm LDK to reduce the active time of IDS in each node of the network.Energy consumption is minimized when Algorithm LDK is used in a mobile network.
- Therefore, it is obvious that to maintain a higher level of security, comparatively more amount of energy needs to be expended.

SYSTEM DESIGN



MODULES LIST :

1. Network formation
2. Attacker
3. PACKET TRANSMISSION
4. LDK algorithm
5. Performance evaluation

MODULE DESCRIPITION:

NETWORK FORMATION

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. A node can be any mobile device with the ability to communicate with other devices

Attacker

We attempt to solve the problem of efficient usage of IDS in two phases: First, we look at the problem from the point of view of a node being monitored by its one-hop neighbors. We present an optimization

problem for the same and analyze it using game theory. Second, we view the problem from the point of view of a node which monitors its neighbors.

Packet transmission

Data packet can be transfer to t he another destination node by the inmternert protocol called as SLAM. The main aim of the protocol is to reduce the time a guard node remains awake for the purpose of monitoring malicious activities. We find that there is an interdependence between the nodes while carrying out network monitoring.

LDK Algorithm

In LDK, the probability with which a node has to monitor depends on the value of the security level. It is defined as the minimum number of neighbors that monitor a node's behavior at any instant. Firstly, the concept of the security level is introduced so that the algorithm LDK can be used in a wide range of application scenarios with varying security requirements.

Performance analysis

In this section we present simulation results for the Algorithm LDK and discuss its performance. We design a cooperative IDS and deploy it in a MANET simulated using simulator and compare its performance under two scenarios.We keep IDSs running on mobile nodes in a network throughout the simulation time.We use the Algorithm LDK to reduce the active time of IDS in each node of the network.

CONCLUSION

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 between the 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 anamolous behaviour, whereas, the secondary goal of the IDSs is to conserve as much energy as possible.

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 and energy resources. In future we wish to extend our model to accommodate a heterogeneous network.

FUTURE ENHANCEMENT

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 and energy resources. In future we wish to extend
our model to accommodate a heterogeneous network.

ACKNOWLEDGEMENT

The author deeply indebted to honorable First and foremost I bow my heads to almighty for blessing me to complete my project work successfully by overcoming all hurdles. I express my immense gratitude to correspondent SHRI A.SRINIVASAN. vice chairman SHRI A.SRINIVASAN(Founder chairman),SHRI P.NEELRAJ(Secreatry)Dhanalakshmi Srinivasan Group of institutions, perambalur for giving me opportunity to work and avail the facilities of the college campus. The author heartfelt and sincere thanks to principal Dr. ARUNADINAKARAN, Vice Principal prof. S.H.AFROZE, HoD Mrs. V.VANEESWARI,(Dept. of CS& IT)Project Guide Mrs. S.SELVAKUMARI, (Dept of CS &IT) of dhanalakshmi Srinivasan College of Arts & Science for women, Perambalur. The author also thanks to Parents, Family Members, Friends, Relatives for their support , freedom and motivation

REFERENCE:

[1] S. Zeadally , R. Hunt, Y-S. Chen, A. Irwin and A. Hassan, ”Vehicular adhoc networks (VANETS): status, results, and challenges,” Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.

[2] S. K. Bhoi and P. M. Khilar, ”Vehicular communication: a survey”, IET Networks, vol. 3, no. 3, pp. 204 - 217, 2014.

[3] S. Marti, T. J. Giuli, K. La and M. Baker, ”Mitigating Routing Mis behavior in a Mobile Ad-hoc Environment,” Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255-265, August 2000.

[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, vol. 4, pp. 3122-3127, October 2003.

[5] K. Nadkarni and A. Mishra, ”Intrusion Detection in MANETs – The Second Wall of Defense,” Proc. IEEE Industrial Electronics Society Conference ’2003, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6, 2003.

[6] 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 8-12, 2005.

[7] N. Marchang and R. Datta, ”Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks,” IET Information Security, vol. 6, no. 4, pp. 77-83, 2012.

[8] N. Marchang and R. Datta, ”Collaborative Techniques for Intrusion Detection in Mobile Ad-hoc Networks,” Elsevier Ad Hoc Networks, vol. 6, no. 4, pp. 508-523, June 2008.

[9] 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,” vol. 22, no. 3, March 2011, pp. 514-527.

[10] I. Khalil, S. Bagchi and N. B. Shroff, ”SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks,” Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007

(DSN 2007), 565-574.

P.kavimozh is presently pursuing M.SC., Final year the Department of Computer Science from Dhanalakshmi Srinivasan College of Arts & Science for Women , perambalur, Tamilnadu.

S.SELVAKUMARI- Recevied M.Sc.,M.Phil Degree in Computer science, She is currently working as Assistant professor in Department of Computer science in Dhanalakshmi Srinivasan College of Arts and science for women, perambalur ,Tamilnadu

K.KASTHURI is presently pursuing M.SC., Final year the Department of Computer Science from Dhanalakshmi srinivasan college of arts &science for women ,Perambalur,Tamilnadu