THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22- Issue-14-December-2019

Effective and Energy Efficient Utilization of Intrusion Detection System in Ad Hoc Networks using Active/Inactive Mechanism

K. Nirmala[1],Dr. Ch.D.V. Subba Rao[2]
[1]Research Scholar, Department of Computer Science and Engineering, S.V University
[2]Professor, Department of Computer Science & Engineering, S V University College of Engineering, S.V University,
Tirupati, A. P., India

ABSTRACT: Mobile Ad Hoc networks are self-organizing networks in which nodes can transfer data between each other by direct connection or by using neighbors node, these nodes runs on battery and to keep them active in network battery life must be efficiently utilized. Mobile Ad Hoc networks can also be attack by malicious nodes to disturb network services; various types of attacks are available such as black hole (in this attack neighbor accepts data from source and drop all packets instead of sending to destination) grey hole (in this attack chosen some packets will be drop and rest sent to destination) worm hole (in this attack neighbor will use another malicious neighbor to transfer data and form a tunnel instead of sending to destination). To avoid such attacks Intrusion Detection Systems are developed and will be run in nodes all the time to monitor nodes behavior, If any nodes dropping packets then this IDS will detect and inform to other nodes about this nodes behavior. Running all the time IDS can consume much battery power and node lifetime can be reduce, to overcome from such issue we introduce concept called Efficient IDS Usage, in this technique a single node with high battery is responsible to monitor behavior of all neighbor nodes in its proximity and other nodes IDS will be in inactive state to save their battery for future use, if selected monitoring nodes energy drop to certain level then another node with high battery will be chosen as next monitoring node. In this paper at the time of network setup all nodes will discover their one hop neighbor and choose one node with high battery as monitoring node and make that node IDS active to monitor them, leftover nodes will be instruct to go to idle or inactive state to save their energy for future use. In a region whatever node sends packet then node with IDS will intercept that packet and perform filteration on that packet to detect abnormal behavior. If packet contains valid data then it

ISSN:0971-1260
Vol-22- Issue-14-December-2019

will forward to destination otherwise packet will be drop at IDS node.

Index terms-Intrusion, attack, sender, receiver, wireless, CCM, CoAP, ADHOP, IoT

1. INTRODUCTION

A wireless AD HOC network or Mobile AD HOC network is a distributed type of wireless network. The network is ad hoc due to its infrastructure less nature, and this network does not require any human effort like wire networks. Instead, each node will act like a sender, receiver or intermediate nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use. Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. Such wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks anywhere, anytime. Each device in an Ad Hoc network allow to move anywhere, and will therefore change its links to other nodes frequently. The primary challenge in building an AD HOC is preparing each node to always preserve neighbor information to correctly route/send packet data. Due to infrastructure less nature this network can be attack and to prevent attack various IDS are introduce but this IDS will run on each node all the time which leads to substantial amount of energy consumption. In this paper we introduce concept to efficiently manage this IDS without losing its effectiveness.

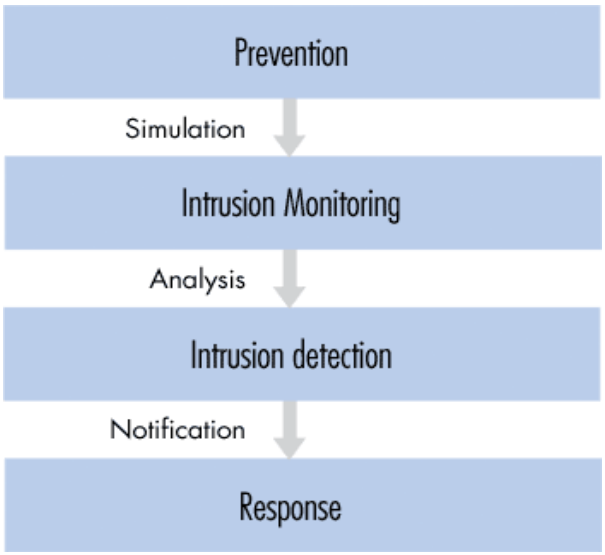

Fig:**Intrusion detection system activities**

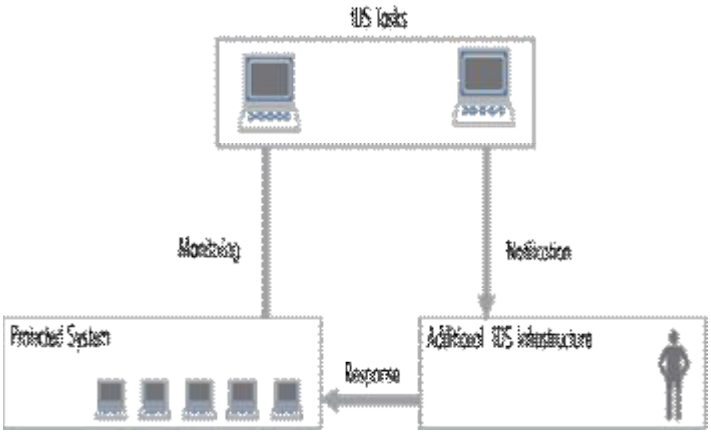

Fig :Intrusion detection system infrastructure

2. LITERATURE SURVEY

ISSN:0971-1260
Vol-22- Issue-14-December-2019

2.1 Energy efficient cross-layer approach for object security of CoAP for IoT devices

CoAP is an application layer protocol designed for resource-constrained devices in Internet-of-Things (IoT). Object Security of CoAP (OSCoAP) is an IETF draft for addressing security issues with CoAP messages that can arise with the use of intermediate proxies. These proxies are employed for better performance, scalability and offloading expensive operations. OSCoAP adopts the counter with cipher block chaining message authentication code (CCM) mode of authenticated encryption with associated data (AEAD) that simultaneously ensures confidentiality, integrity, and authentication of the messages. The current implementation of CCM for OSCoAP is carried out in software. In this paper, we propose a cross-layer approach towards exploiting the CCM for OSCoAPusing mac-layer security suite in IoT devices. The motivation is based on the fact that most of these devices are equipped with 802.15.4 radio chips. The IEEE 802.15.4 standard mandates the availability of some security features for mac-layer encryption in these radio chips including the CCM. We propose an algorithm that takes advantage of these on-board features by efficiently implementing the CCM operations for OSCoAP. The results show that our implementation of CCM is memory efficient, save up to 10 times more energy, improves battery life by 30% and is 37% faster than state of the art software implementation of CCM for OSCoAP.

2.2 ADHOP: An energy aware routing algorithm for mobile wireless sensor networks

Sensor node typically features an embedded processor, a limited memory, and a low-power wireless radio [5]. Furthermore, such devices are typically battery powered, thus imposing several restrictions on the design of protocols for WSNs [1], [10], from the physical to the application layer. Maximizing the network lifetime and balancing the energy consumption have raised some attention and effort on several approaches of routing in Wireless Sensor Networks (WSNs). Hence, many proposals for routing protocols have specifically been made to handle energy depletion, although few consider mobile sensor nodes [3], [7]. However, dealing with the limited energy resources of sensor nodes, in mobile WSNs, becomes a considerable challenge in the design of routing protocols. Ant-based routing algorithms use pheromone

ISSN:0971-1260
Vol-22- Issue-14-December-2019

to learn and adapt routes in relatively short periods. Nevertheless, most of them are not suitable for low-power wireless networks [7]. Such algorithms typically use control packet transmissions in order to keep the pheromone information updated and to establish reliable data delivery ratio. However, in WSNs, a routing protocol must avoid additional routing overhead as much as they must distribute the load transmission over the network in order to save residual energy in the nodes. Therefore, energy aware routing protocols must dynamically handle network topology changes while they must also be energy efficiency. In this work, we introduce an energy aware Ant-based Dynamic Hop Optimization Protocol (ADHOP), a self configuring and multihop reactive routing protocol which aims at providing a low-overhead routing for mobile WSNs. Our approach uses the ant collective behavior to make routing decisions by pheromone and heuristic information. By using pheromone, ADHOP can adapt to network changes, such as mobility and node failures. In fact, ADHOP is designed to use one or more heuristic information to support routing decisions according to the network needs, such as distance, latency, residual energy, and/or Received Signal Strength Indicator (RSSI). Our approach aims at using residual energy information to distribute the network traffic load, thus reducing the energy consumption per delivered data.

3. SYSTEM ANALYSIS

3.1 Existing System

All existing Ad Hoc network nodes are equip with IDS to monitor mobile/nodes activity and the main task of IDS is to filter packet to look for malicious activity, if any such activity detected then packet will be drop to save network, this IDS will run on each and every node and consume 25% of mobile, this much battery consumption can cause network to die soon and we need to utilize IDS and its energy consumption efficiently in order to increase network life time.In utmost of the prevailing IDSs for Ad Hoc Networks, a monitoring system sits at each node, which runs all the time. One collective mechanism used by these IDSs is to detect/monitor packet data in the node's neighboring area. Since a node in an Ad Hoc might have restricted battery power and computational resources, running an IDS all the time may turn out to be a costly overhead. Thus, the challenge is how to calculate how many IDS needs to remain active without compromising its effectiveness. This question may not be much of a worry in a wired network, in which an IDS is installed

ISSN:0971-1260
Vol-22- Issue-14-December-2019

mainly in a stationary router or gateway, with virtually unlimited computational and battery power. However, this is of important concern in the case of Ad Hoc, where the mobile nodes themselves not only behave as hosts and routers but have to carry out other functions as well, such as intrusion detection either collaboratively or individually. To this end, we propose a distributed scheme for efficient usage of IDSs.

Disadvantages

Run IDS on all nodes all the time, which consume much energy of each node

No existing technique or algorithm implemented for efficiently management of IDS.

3.2 Proposed System

For effective and efficient utilization of IDS we have introduce node active/inactive concept in which at the time of network setup one hop with high battery will be appointed as monitor node and make that node IDS to be in active state and other nodes IDS in that region will be inform to go to inactive state to save their energy for future use. If monitoring node battery level drops to certain level then we network will appoint new node as monitor with high battery level, by applying this technique we can save 30% of network life time and can manage IDS efficiently.

The contributions of this paper are summarized as follows.

1) We present an innovative technique, which is based on a node IDS active/inactive state, to optimize the active time duration of IDSs in an Ad Hoc networks. This technique reduces the IDSs' active time as much as possible without compromising its effectiveness.

2) To certify our recommended method, we also present a multiplayer cooperative game that analyzes the effects of individual IDSs with reduced activity on the network.

3) With experiments, we proved that substantial savings in computational cost and energy is achieved with our given technique of optimize/enhancing the active time of the IDSs while sustaining the performance of the Intrusion Detection System.

4) This technique making use of local information, thus making it distributed and scalable. Additionally, this technique can be applied on both mobile and static networks.\

Advantages

ISSN:0971-1260
Vol-22- Issue-14-December-2019

Single IDS will be running on selected high battery node in a region to monitor activities of other nodes in that region, other node IDS will be in inactive state to save energy for future use.

Automatically switch to another node for monitoring the network when current monitor node energy drops down.

Can increase network lifetime up to 30% compare to existing technique.

4. CONCLUSION: In this paper, we have analyzed for effective and efficient utilization of IDS using node active/inactive concept. So, we can save 30% of network life time and can manage IDS efficiently.

REFERENCES

[1] E. Ahmed, K. Samad, and W. Mahmood, "Cluster-based intrusion detection (cbid) architecture for mobile ad hoc networks," in 5th Conference, AusCERT2006 Gold Coast, Australia, May 2006 Proceedings, 2006.

[2] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," in Wireless Network Security, pp. 159–180, Springer, 2007.

[3] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," in Applications and the Internet Workshops, 2003. Proceedings.2003 Symposium on, pp. 368–373, IEEE, 2003.

[4] M. Ngadi, A. H. Abdullah, S. Mandala, et al., "A survey on manet intrusion detection," International Journal of Computer Science and Security, vol. 2, no. 1, pp. 1–11, 2008.

[5] A. Nadeem and M. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," 2012.

[6] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1, pp. 38–47, 2004.

[7] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," Wireless Communications, IEEE, vol. 14, no. 5, pp. 56–63, 2007.

[8] D. Choudhury, D. Kar, K. R. Biswas and H. N. Saha, "Energy efficient routing in mobile ad-hoc networks , " in proc. of 6th International Conference and Workshop on Computing and Communication (IEMCON -2015), IEEE Xplore Digital Library, October 2015 , pp. 1-7.

ISSN:0971-1260
Vol-22- Issue-14-December-2019

[9] S. Doshi and T. X. Brown, "Minimum energy routing schemes for a wireless ad hoc network," in Proceedings of the Conference on Computer Communications (IEEE Infocom '02), 2002.