INTRODUCTION TO INTRUSION DETECTION SYSTEMS IN MOBILE AD HOC NETWORKS: STATE OF THE ART

Mohamed Elboukhari¹, Mostafa Azizi¹ and Abdelmalek Azizi²,³

¹Department of Applied Engineering, ESTO, Oujda, Morocco
²Department Mathematics & Computer Science, FSO, Oujda, Morocco
³Academy Hassan II of Sciences & Technology, Rabat, Morocco

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are more vulnerable to different attacks. Prevention methods as cryptographic techniques alone are not sufficient to make them secure; therefore, efficient intrusion detection must be deployed and elaborated to facilitate the identification of attacks. An Intrusion Detection System (IDS) aims to detect malicious and selfish nodes in a network. The intrusion detection methods used normally for wired networks can no longer adequate when adapted directly to a wireless ad-hoc network, so existing techniques of intrusion detection have to be changed and new techniques have to be determined to work efficiently and effectively in this new network architecture of MANETs. In this paper we give a survey of different architectures and methods of intrusion detection systems (IDSs) for MANETs accordingly to the recent literature.

KEYWORDS


1.INTRODUCTION

In most enterprise environments security actually is based on the approach of defense-in-depth, where several layers of defenses are employed to prevent attackers from violating the security policies of the enterprise. This approach is concerned on the premise that, even if an attacker penetrates certain layers of defense, he can not cause much harm because the other layers will provide protection.

The technology in traditional wireline networks that is employed as a first layer of defense at the perimeter of the network is a firewall. Firewalls are employed to prevent outsiders from penetrating the enterprise network. Cryptography methods are another technology being employed as a preventive layer to keep outsiders from accessing sensible resources.

Even though these methods present a formidable barrier to attackers, an additional layer of defense called intrusion detection is often employed to protect networks. Intrusion detection system (IDS) concentrates on detecting malicious activity from attackers that have successfully penetrated the perimeter defenses.

Several researches have already been carried out in intrusion detection for traditional wired networks. Implementing the research of wired networks to wireless networks however is not an easy task because of key architectural differences. Due to their vulnerabilities, mobile ad hoc networks (MANETs) provide a tougher challenge for designing an IDS.

DOI:10.5121/ijcsa.2015.5203
MANET has emerged as a new technology to provide anytime, anywhere communication. Increasingly wireless ad-hoc networks are being employed in the tactical battlefield, emergency rescue and search missions, as well as civilian ad-hoc situations like classrooms and conferences. This is due to the speed and ease in setting up such networks. Wireless ad-hoc networks have different characteristics from a wired network, such as open medium, dynamic topology, limited bandwidth and limited power. The use of MANETs in recent years has been used in many applications, including some critical applications, and as such security has become one of the major goals in MANETs.

In this paper we provide a survey of methods used to implement intrusion detections systems (IDSs) in MANETs environment. The organization of our article is as follows. Our survey of methods to implement IDSs in MANETs is presented in section 2. We conclude our article in section 3.

2.EVOLUTION OF INTRUSION DETECTION SYSTEMS FOR MANETS

In this section we give a survey on IDSs for MANETs. Mainly, we will present essentially the well-known techniques used for IDSs according to the recent literature.

Two methods were elaborated in 2000 by Marti et al. [1], Watchdog and Pathrater, to be added on top of the routing protocol DSR (Dynamic Source Routing [2]) in MANETs. The Watchdog determines the misbehaving nodes by eavesdropping on the transmission of the next hop, while the Pathrater aids to find the routes that do not contain those nodes.

A Knowledge-based IDS was proposed [3] in 2001, which use knowledge about attacks, study traffic and try to determine patterns indicating that a suspicious behaviour is occurring. This approach may be employed against known attack patterns only. These IDSs are important because of their low false alarm rates and high accuracy. A real-time knowledge-based network IDS for detecting link-state routing protocol attacks has been described specifically for OSPF.

In 2002, K.Paul et al. presented an approach [4] that employs hash chain in route discovery process and an observer to sensor attacks of the neighbour station and then neighbour report the behaviour of the station to source station which determines the rating for the accessed station and this rating is employed to decide the malicious station.

Albers et al. [5] elaborated in 2002 a collaborative and distributed architecture of IDS by using mobile agents. On every node, a Local Intrusion Detection System (LIDS) is implemented for local concern that can be extended for global concern by cooperating with other LIDS. Two kinds of data are exchanged among LIDS: intrusion alerts to inform others of locally detected intrusion and security data to obtain complementary information from collaborating nodes. Information must be obtained from what LIDS detects, with additional data from other stations in order to study the possible intrusion.

Similar to Watchdog and Pathrater scheme, another approach called CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Networks) [6] has been proposed in 2002 to overcome the drawbacks of the Watchdog and Pathrater by ignoring misbehaving nodes in the routing process. Based on trust, every node identifies its neighbours as enemies and friends. Also, friends are informed of enemies.
In the same year, Michiardi and Molva [7] described a method called CORE (a Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks) to sense a specific kind of misbehaving stations, which are selfish stations, and also obliged them to cooperate.

OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) [8] was presented as another extension to the DSR protocol in 2003. Also, OCEAN employs a reputation system and a monitoring system. The implemented solution relies only on its own monitoring to avoid false accusation from second-hand reputation exchanges. The false accusation presents the new vulnerability. Therefore, OCEAN implements a stand-alone architecture.

In 2003, O. Kachirski and R. Guha elaborated a sensor based approach to detect intrusion. The multiple detectors are implemented and audit data is collected from all the sensors these data is merged to sense the intrusion [9].

In the same year, the Farooq Anjum et al. presented a “signature based intrusion detection technique”, in which they assume that they recognise the signature of the attack and all the system run the IDS such stations are said to present the intrusion detection subsystem [10]. Bo Sun et al. in [11] elaborated a non-overlapping Zone- Based Intrusion Detection System (ZBIDS) that fits the requirement of MANETs. They present details of implementing the Markov Chain based local anomaly detection model, having feature extraction, detection engine construction, parameter tuning, and data pre-process. The whole network is organized into non-overlapping zones. There are two types of nodes in ZBIDS, if one station possesses a physical connection to a station in a different zone; this station is named a gateway station. Otherwise, it is referenced as an intra-zone node. Only gateway nodes can initiate alarms. They use the local alerts broadcast from the intra-zone stations and execute correlation tasks and aggregation to remove many falsified alerts.

D. Sterne, et al. in 2004 present a cooperative intrusion detection architecture [12] that facilitates accurate detection of MANET-specific and conventional attacks. The architecture is considered as a dynamic hierarchy in which detection information is captured at the leaves and is aggregated, analyzed, and reduced as it passes upward toward the root station. The nodes at the top of architecture are responsible for security management functions.

In 2005, Ioanna Stamouli presented RIDAN architecture which employs timed finite state machine to determine malicious misbehaviours against the AODV routing protocol. It employs a knowledge based methodology to detect the intrusion [13]. RIDAN operates locally in every participating node and monitor the network traffic. This model can detect resource consumption attack, Sequence number attack and dropping routing packet attack.

In 2006, SCAN [14] is implemented on two central ideas. First, each node monitors its neighbors for packet forwarding or routing misbehaviour, independently. Second, by cross validating the overhead traffic with other nodes, every node observes its neighbours. By a majority decision, Nodes are declared malicious. This supposes that the network density is sufficiently high. But in SCAN the services of network are temporarily stopped during the intrusion detection phase. The detection efficiency is reduced by the lack of mobility. The assumption that network density is high cannot always hold. The increase in mobility results in higher false positives. The packet delivery ratio also can be heavily affected in the interval during which an attack is started and when it is detected. The communication overhead also increases with the increase in the percentage of malicious stations and with mobility.
In the same year, A. Karygiannis et al. elaborated a method to sense the critical station for MANET [15]. Critical station is a station whose failure or malicious behaviour disconnects or degrades the network. After identification of critical node, these nodes are monitored continuously. To detect the critical node they employed a vertex cut and edge cut approach. A vertex-cut is a set of vertices whose removal generates a sub graph with more components than the original. To decrease the number of critical station, tests are performed. A lightweight trigger service monitors network traffic and begins a critical station test when it detects such a condition can exist. The trigger service is implemented to allow false positives that the critical station test will later screen out. The trigger service monitors the number of connections served by the test station and the number of packets traversing the test station. Also, the trigger itself can operate as a lightweight alternative to the critical station test.

In [16] S.Bose et al. presented a “Neural network approach for anomaly intrusion detection in ad hoc network using mobile agents”. In this paper they employ mobile agents that interact with machine, collect information. They employed the user log file data generated from local host for training the neural network for the purpose of intrusion detection. Their system obtains high intrusion detection rate and low false alarm rate.

Xia Wang presented an end to end Wormhole detection method in wireless ad hoc networks [17]. He used AODV protocol. In the route discovery process the sender node sets the Destination-only flag such that only the destination node can respond to the ROUTE REQUEST message. When the ROUTE REQUEST message received by the destination node, it responds by transmitting a ROUTE REPLY with its current position. The sender obtains position of the receiver from the ROUTE REPLY message and determines the lower bound of hops between the sender and the receiver node. The corresponding route will be eliminated if the received route is shorter than the estimated shortest path,. Otherwise, the sender will choose the shortest path corresponding to the estimation. After the detection of wormhole by the sender node, it enables temporarily the path with wormhole and transmits the TRACE message to the receiver through this path. The TRACE message is transmitted by each intermediate station through the route with wormhole. Any station on the route receives the TRACE message, it responds to sender by transmitting its current position and hop count to the destination station. The sender node may measure the increase of hop count at each station employing the received position. If the augmentation of hop count at one station is not one comparing to its previous hop, then this station and its previous hop station are concerned as the wormhole.

Yu Liu et al. presented a Bayesian Game Approach for IDS in MANETs [18]. In this article, they implemented a game theoretic framework to study the interactions between pairs of attacking/defending stations employing a Bayesian formulation. They analysed the achievable Nash equilibrium for the attacker/defender game in both static and dynamic scenarios. The dynamic Bayesian game is a realistic model, because it allows the defender node to update his belief on his opponent’s maliciousness as the game runs. A new Bayesian hybrid detection approach is presented for the defender node, in which a lightweight observing system is employed to determine his opponent’s actions, and a heavyweight observing system acts as a last resort of defense. The difference between a dynamic and a static Bayesian game is that the former does not suppose the game evolution and the defender has rigid prior beliefs about the kinds of his opponent. In contrast, the latter is a more realistic game model; since the defender node may
dynamically update his beliefs based on new detections of the opponent’s actions and the game history, and then may update his observation strategy accordingly. The advantage of implementing the IDS system as a Bayesian hybrid IDS is that it aids to save significant energy (potentially spent on continuously monitoring the network), while minimizing the potential damage infected by an undetected attacker. This provides an important property of the equilibrium solution: the monitoring probability does not depend on the current belief of the defender node, but rather influences the attacker behaviour.

J Martin et al. in 2006 presented a secure routing approach called Resiliency Oriented Secure (ROS) which contains the detection phase in routing to sense the malicious node [19]. To sense the malicious station, they employed some updates field in the routing table and set some threshold value for it. Whenever any station receives a routing message that has an update in its own routing table, it increments the number of update field by one. When the count values crosses the threshold values it triggers alarm signal. R. Ranjana et al. in the year 2007 described a model which does not do any change in underlying protocol and employed additional security component to sense resource consumption attack, fabrication attack and packet dropping attack [20].

Using an extended architecture, IDSX [21] is a cluster-based solution and it acts as a second line of defense. Any IDS solution could be implemented by individual nodes. The IDSX is compatible with any intrusion detection system operating as the first line of defense. The IDSX hardly produced any false positives according to the simulation results. IDSX forms a consensus of the responses from several individual IDS solutions operated in the stations. Anomaly-based intrusion detection schemes could be implemented as the first line of defense. The IDSX works within preset boundaries. These are quite practical and feasible enough considering the nature of ad hoc networks. The elaborated two-step approach can make the task of intrusion detection service very expensive.

In [22] eSOM is presented employing the concept of unsupervised learning in Artificial Neural Networks employing Self-Organizing Maps. The technique used a data structure called U-matrix which is used to represent data classes. These regions represent malicious information and are watermarked using the Block-Wise method. The regions representing the benign data class are marked using the Lattice method. When a new attack is initiated it causes changes in the pixel values. The Watermarking technique and eSOM can together identify if any pixel has been modified and this makes it very sensitive towards detecting intrusions. Using eSOM, the IDS would be trained in regular time periods. This takes a toll on the energy efficiency of the algorithm and results in additional overhead. But the proposed intrusion detection service has not been employed on different routing protocols.

Ningrinla marching et al. presented an IDS [23]. They described two intrusion detection methods for MANETs, which employ collaborative efforts of stations in a neighbourhood to sense a malicious behaviour in that neighbourhood. The first technique is proposed for detection of malicious nodes in a neighbourhood of nodes in which each pair of nodes in the neighbourhood are within radio range of each other and such a neighbourhood of nodes is known as a clique. The second method is presented for detection of attacks in a neighbourhood of stations, in which each pair of stations can not be in radio range of each other but where there is a station among them which has all the other stations in its one-hop vicinity. This neighbourhood is identical to a cluster. Both techniques employ message passing between the nodes. A node called the monitor node performs the detection process. Based on the packets it receives during the detection service, each station can know the station it suspects to be an attacker and transmit votes to the monitor station. The monitor station upon inspecting the votes precises the malicious stations among the suspected stations. This IDS is independent of any routing protocol.
Pasquale Donadio et al. [24] presented a Grid based Intrusion Detection System (G-IDS) that employs the basic techniques of the Grid computing and apply them to the IDSs, in order to determine a new process capable to protect networks with changing of the topology. They employed a distributed traffic analyser that operating in real-time feedback sharing the results between the neighbouring stations of the network.

S.Madhavi and Dr. Tai Hoon Kim [25] proposed a mobile Intrusion Detection System for multi-hop ad-hoc wireless network in their work. The authors define the monitor node which detects misbehaving node. Also they described the algorithm for sensing packet delaying attack and the packet dropping.

A leader election for intrusion detection system in Mobile Ad Hoc Networks based on the Vickrey, Clarke and Groves (VCG) model was elaborated [26]. The model considers every station to be as honest as possible and leaders are chosen in a way which results in optimal resource employment. For participating honestly in the election process, leaders are positively rewarded. A higher effective lifetime of the stations was accomplished by balancing the resource consumption amongst the stations. Experimental results describe show how the VCG model works well during leader election by giving a higher percentage of alive stations. But the experimental results show that the normal stations die faster when selfish nodes exist in the network. The model elects the same node as leader repeatedly in the case of static scenarios and this causes the normal nodes to die very fast.

Another approach to the IDS has been proposed in [27] and it is called HIDS. This technique is based on reputation or trust or honesty values of the mobile nodes. Depending on its behaviour, the trust value of a node is dynamically increased or decreased. If a station acts normally, it is positively rewarded; malicious behaviour generates negative rewards for the same station. The trust on a node is recalculated based on the rewards that it has earned, and its current honesty rate. Inherently HIDS is protected against false positives. But maintaining routing tables at different stations can not be an energy-efficient strategy. The proposed HIDS also offers only a generic architecture for secure route detection.

Hadi Otrok et al. in [28] treat the problem of increasing the effectiveness of an IDS for a cluster of stations in MANETs. To decrease the performance overhead of the IDS, a leader node is usually chosen to implement the IDS on behalf of the whole cluster. To augment the effectiveness of an intrusion detection system service, they present a unified framework that is capable to: (1) Equilibrate the resource consumption among all the stations and thus augment the life a cluster by choosing truthfully the most cost-efficient station known as leader- IDS. A mechanism is elaborated using Vickrey, Clarke, and Groves (VCG) to achieve the desired goal. (2) Catch and punish a misbehaving leader through checkers that observe the behaviour of the leader. A cooperative game-theoretic model is described to study the interaction among checkers to decrease the false-positive rate. A multi-stage catch mechanism is also described to reduce the performance overhead of checkers. (3) Optimize the probability of sensing for an elected leader. This is implemented by formulating a zero-sum non-cooperative game between the intruder and leader. They give solution to the game by finding the Bayesian Nash Equilibrium where the leader’s optimal sensing detection strategy is precised. Finally, empirical results are provided to support their solutions.
S. Sen et al. elaborated a “grammatical evolution approach to intrusion detection on mobile ad hoc networks”[29]. They employ artificial intelligence based learning technique to explore design space. The grammatical evolution method is employed to sensor known malicious behaviour on MANETs such as Denial of Service (DOS) attacks. IDS are used for each attack and distributed to each station.

A hybrid solution described in [30] combines the Watchdog and Pathrater scheme has been proposed by Martí et al. and SCAN [14]. Nevertheless, neither SCAN nor Watchdog and Pathraters address the mobility issue that well. Also, this hybrid solution suffers from the same problems. There are no fixed stations which can behave as umpires. There must be some type of a leader election model that runs in every node to choose the Umpire nodes. This results in energy consumption and an increased overhead. The authors did not precise the scenario where Umpire nodes themselves can become malicious.

In the elaborated method [31] the authors’s aims to employ one of the danger theory intrusion detection algorithms named the dendritic cell algorithm (DCA). DCA is used to sense the sleep deprivation attack over Mobile Ad Hoc Network. DCA is implemented in a mobile dendritic cell algorithm named MDCA. Each station can protect itself from danger locally. At the beginning, the algorithm controls each entered packet’s ID in the memory. If the packet ID is viewed in the detected list, this involves it comes from a detected attacker, the method rejects the packet, removes its data from the routing table and transmit an alarm to other stations. Else if the packet ID is viewed in the alarmed list, this shows the packet sends by an attacker detected by another station, hence it is removed from the routing table without sending alarm. Else, the packet must be treated by the packet analyser which extracts the required antigens from the routing table and generates the signals from the routing table, the availability of the bandwidth, and the power consumption rate. The packet analyser at the end maintains the signals and antigens in the signals and antigens stores respectively.

A black hole is a station that alternately can execute a black hole attack or can act as a normal node. In [32], IDS nodes are implemented in MANETs in order to avoid and sense black hole attacks.

The objective of the leader election is to extend the lifetime of a MANET by balancing the resource consumption among all nodes. The nodes with more remaining resources should be chosen as the leader. There are however two main complication in attained this objective. In order to not serving others, a station can lie about its remaining resources to avoid being elected [33].

Alert aggregation is an important associate task of intrusion detection. The goal is to precise and to cluster dissimilar alerts generated by small level IDSs, firewalls. As performed new method for online alert aggregation [34], this technique is dependent on a probabilistic, dynamic model of the current attack situation.

In the reference [35] the authors implemented a hybrid technique based on negative selection (NS) and the artificial bee colony (ABC) methods, known as BeeID. The method divided in three phases: training, detection, and updating. During the training phase, a niching artificial bee colony algorithm, named Niche NABC, implements algorithm several times to derive a set of sensors to cover the non self space. During the detection phase, sensors are used to differentiate between malicious and normal network activities. The set of sensor in the updating phase is updated by one of two methods of total updating or partial updating. They employ the Monte Carlo integration to calculate the amount of the nonself space covered by sensors and to specify when the total updating can be done.
Intrusion detection is employed as a successive line of protection in MANETs. To carry out the protection they implemented five supervised [36] categorization algorithms for intrusion exposures method. They calculate their performance on a dataset including different states mobility model and traffic for several attacks.

In [37], authors described and executed a fresh intrusion detection method Enhanced Adaptive Acknowledgment (EAACK) particularly intended for MANETs. EAACK does not degrade the network performances. It is recognized as elevated attacks.

An IDS for MANETs in [38] is elaborated that sensors different attacks and provides an efficient reply. It does not affect the network performance. They consider the deficiencies of a static response to an attack and remove the deficiencies with a flexible response.

An IDS [39] have been developed for isolation of attacks. The MAC layer will be employed for detecting malicious behaviors and will concentrate on the detecting of attack sequences in the network. The Cognitive radio network is used to detect attacks, a simple and effective IDS is then proposed [40]. They showed non-parametric cumulative sum as they modify the point of detection.

3. CONCLUSIONS

Wireless networks are increasingly developed for situations where fixed infrastructure networks are not practical. Nevertheless, with this flexibility comes an additional security burden. Intrusion prevention as using cryptographic techniques is not always practical, so intrusion detection becomes an important second line of defense. Recently, there has been a significant amount of research on this topic. The application of intrusion detection systems to wireless ad hoc networks is a recent development. Wireless ad hoc networks have a limited resources ad this add several challenges to the design of IDS. IDS schemes which need analysis a large data employed by misuse detection methods are not suitable.

In this paper we have reviewed different techniques and methods used to implement IDS in MANETs. We tried to mention several works to show the difference between the methods employed. We consider that our work is useful for researchers concerned with the IDS in MANETs environment, especially our review is elaborated according to the recent literature. In the future, we will illustrate the advantages and disadvantages of different methods of IDS, also we will give comparison between these different techniques.

REFERENCES


[33] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabin Bhattacharya —Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET1, IEEE transactions on dependable and secure computing volume: 8, issue: 1 2011 , page(s): 89 - 103

[34] Alexander Hofmann, Bernhard Sick, Member, —On-Line Intrusion Alert Aggregation with Generative Data Stream Modeling1, IEEE Transactions on Dependable and Secure Computing, (Volume: 8, Issue: 2), March-April 2011


Authors

Mohamed elboukhari received the DESA (diploma of high study) degree in numerical analysis, computer science and treatment of signal in 2005 from the University of Science, Oujda, Morocco. He is currently an assistant professor, department of Applied Engineering, ESTO, university Mohamed First, Oujda, Morocco. His research interests include cryptography, quantum cryptography and wireless network security, Mobile Ad Hoc Networks (MANETS).

Mostafa azizi received the diploma of engineer in automatic and computer industry in 1993 from school Mohammadia of engineers, Rabat, Morocco and he received the Ph. D in computer science in 2001 from the university Montreal, Canada. He is currently professor at university of Mohamed first, Oujda, Morocco. His main interests include aspect of real time, embedded system, security and communication and management of the computer systems in relation with process industry.

Abdemalek azizi received the Ph. D in theory of numbers in 1993 from university Laval, Canada. He is professor at department of mathematics in university Mohamed First, Oujda, Morocco. He is interesting in history of mathematics in Morocco and in the application of the theory of number in cryptography.