International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Detection and Localization of IDS Based Spoofing Attackers in Wireless Sensor Networks

Ankit Singh[a]*, Pallav Sinha[b], Soumyajyoti Bhattacharya[c]

[a]*University of South Florida,Tampa and United States of America*
[b]*Cognizant, Chennai and India*
[c]*IIT Kharagpur, Kharagpur and India*
[a]*Email: singhankit0803@gmail.com*
[b]*Email: sinhapallav19@gmail.com*
[c]*Email: soumyajyotib909@hotmail.com*

Abstract

A Wireless sensor network consists of a series of sensing devices. These track parameters such as those required for tracking and surveillance and then effectively passes on this information with other such sensors over a specific geographical area within the wireless network. The problem with traditional wireless networks lies in the way that they are positioned in an unattended manner, being controlled remotely by the network operator. This opens up a pathway for attackers, which compromise and capture wireless nodes and launch a variety of attacks that impair the functioning of the system. The proposed system aims to localize and cluster these nodes together, according to their position, wherein the cluster head acts as an Intrusion Detection system by monitoring node behavior such as packet transmission. This information is used to identify the attacked nodes in the wireless sensor network.

Keywords: K-Means Clustering; Intrusion Detection System; Packet transmission; Networks; Cryptography.

1. Introduction

Wireless sensor networks have always been prone to a variety of attacks that compromise its performance such as spoofing attacks. A spoofing attack is one in which a program or in some cases a person successfully disguises itself as another by manipulating data and taking illicit advantage.

---

* Corresponding author.

In a large- scale network, multiple adversaries may group together to launch potent attacks such as Network Resource Utilization attack and Denial-of-Service attack which cripple the performance of the network. The proposed system introduces an Intrusion detection system at the cluster head that will proceed to reduce attacks by a localized elimination system. The approaches taken by people in current existence that have been introduced to prevent spoofing attacks are mostly all based on cryptographic schemes. However cryptographic schemes are not the best suited for such purposes as they require large infrastructural, computational and management overhead. Cryptographic schemes are based on secure distribution, maintenance and management mechanisms for keys and the small sensors generally have memory and computational constraints. This warrants an alternate approach, and the use of RSS-based spatial correlation and a node associated physical property, which is almost impossible to falsify, presents this opportunity. Spatial correlation is employed to recognize any spoofing attacks which are happening and also to restrict adversaries to local scenarios, without any additional costs or modification to the existing wireless sensor network.

2. Problem Statement

Wireless networks are widely used as they have proved to be a simple and effective means of communication. However, their open medium and mobility leaves them vulnerable to various kinds of attacks that degrade network performance. The existing protocols that are used to protect them, such as WEP, WPA and WPA 2 are however susceptible to spoofing attacks which can be performed with minimal effort such as a change of MAC address in 802.11 networks. The conventional methods of using cryptographic schemes also have limited scope due to the huge computational overhead that distributing, maintaining or indexing cryptographic keys require. This warrants the need for an alternative approach, one that presents data that is hard to falsify, while at the same time adding no additional cost or requiring any modifications to the existing network.

2.1. Disadvantages of Existing System

The existing system presents a lot of problems that needs to be addressed.

- Low cost sensors are incapable of creating and studying detection log files due to a limited memory budget and computational capabilities.
- The large network size and infrastructure less architecture makes it impossible for a base station to collect audit data from the whole network
- Static MAC address makes it easier for launching attacks.

3. Related Work

3.1. Impact of Sampling Number and Threshold Value

As shown by the works of Jie Yang, Yingying Chen, Wade Trappe in [1] and also by M.Bohqe and Jerry Chenq in [2], thresholds are determined based on parameters such as power transmission and energy values. These threshold values outline the critical region for the significance testing. If the threshold value is set appropriately, it allows the attack detection mechanism to be robust to false detections. A curve showcasing variation of

cumulative distribution function, Dm against the threshold value is plotted. It is observed that the curve of Dm shifts greatly to the right in case of a spoofing attack. Thus, when the Dm value exceeds the threshold value, the presence of an attack is confirmed.

3.2. IDS Classification

As highlighted by the works of M.Loganathan and V.Navaneethakrishnan in [4], Intrusion Detection Systems can be broadly classified as belonging to two categories, network-based and host-based IDS. Network based systems actively or passively listen on the network while capturing and examining individual packets. NIDS can analyze the entire packet and not just IP addresses and ports. They can observe the packet induced payload, to analyze the host application being accessed and raise an alarm when the exploitative practices of the attacker sets in with respect to the code. Network IDS are host independent and cover entire networks of systems. On the other hand, host-based IDS are concerned with activities occurring on each individual host. They can detect actions such as repeated failed access attempts or changes to critical system files. Moreover, they operate by accessing log files or monitoring real-time system usage**.**

3.3. Issues in Wireless Networks

Referenced from the works of V.Brik, S. Banerjee, M.Gruteser and S.Oh in [6]. All communications in wireless networks are carried on in an open environment which makes it difficult to monitor traffic of the network in question at various checkpoints. Hence, in ad-hoc networks, network monitoring is performed at every network node [7]. This consumes a lot of bandwidth and needs a lot of processing power. In the case of host-based monitoring, a greater amount of processing work is required to be done on each host. This in turn reduces the battery life and slows down the host considerably.

4. System Architecture

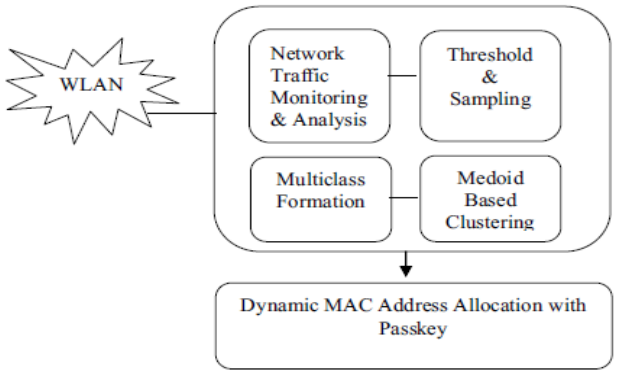


Figure 1: System Architecture

The existing method for preventing attacks is shown in the figure. It is based on dynamic allocation of MAC address. The proposed system builds upon the already existing system and adds a few modules that together

make it a more robust and efficient system for preventing spoofing attacks by identifying the attack, evaluating the number of attackers and localizing and eliminating these adversaries. The fundamentals on which the model functions include:

- RSS based analysis and Medoid based clustering: The received signal strength is a physical property that is closely correlated with locations in the physical space. Each node is given RSS positions as (x,y) coordinates according to their spatial position or physical location in space. This data is then stored and used for analysis and helps in localizing the victim nodes.
- Medoid based clustering: The algorithm employed here is the k-medoids algorithm which is a clustering algorithm similar to k-means and medoidshift algorithm. A medoid is classified as the object in a cluster whose average dissimilarity to all other such objects is the least, thus making it that specific point in the cluster which is most centrally positioned. The k-medoids algorithm is partitional in nature and chooses datapoints, called medoids as center. It works on the generalization of Manhattan Norm to classify distance between datapoints. On the basis of the analysis above, a threshold value was set up. This value helped in determining attack occurrence [9].
- Node Authentication and Dynamic MAC address assignment: In order to prevent spoofing attacks, MAC addresses were dynamically allocated. This makes it tougher for the adversary as the MAC address keeps on changing during the course of the attack. Furthermore, a dynamic MAC address would be designated based on threshold values. Each node needs to be authorized using a passkey and a special Dynamic Allocation MAC, DAM table was established for conserving the Dynamic MAC address logger as well as the passkey value of the node [10].

5. Approach and Evaluation of Proposed System.

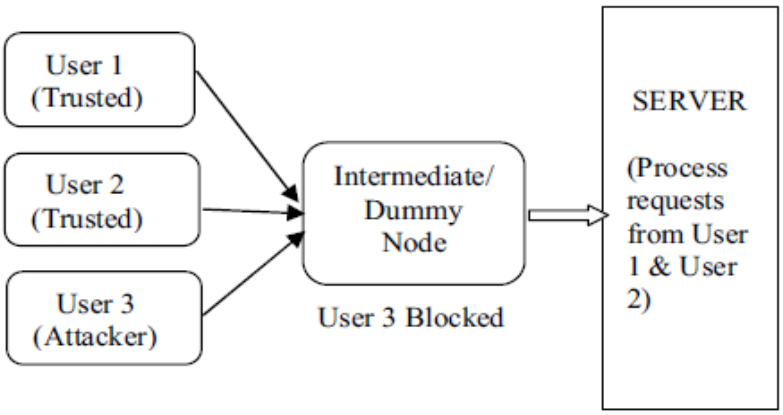
The proposed model introduces four modules, each performing their own function but coming together in a cohesive manner to perform the tasks of detecting an attack, finding out the number of attackers and localizing them. These modules are described at length as under:

- Traffic Reducing System: In a typical wireless sensor network, multiple requests to the server are made from trusted as well as attacker nodes. This means that there would be huge traffic on the server to process requests from the users, which would in turn slow down the performance of the server. For prevention of an attack and also to reduce traffic, the proposed system introduces an intermediate node. This intermediate node would act as a proxy lying between the server and the users. The users believe that they are sending direct requests to the server but in reality, their requests are being redirected to the intermediate node, which acts as a proxy and filters the requests as they are received [11]. The intermediate node determines the number of data requests from various nodes and then sends them accordingly to the server so that the server could respond to them immediately. This method ensures optimal performance of the server which can respond to responses from trusted nodes immediately, while at the same time avoiding requests from compromised nodes.
- Attack detection and its localization by K-Means approach: This is based on the concept of Received Signal Strength or RSS and is measured across a set of access points to perform detection and

localization of spoofing attacks. RSS is the signal strength of a received frame measured at the receiver's antenna. It is a measurement that is difficult to falsify randomly, as it heavily relies on the location of the transmitter. Several commercial 802.11 networks present frame by frame RSS measurements. In turn, RSS is directly in relation to the transmission power, the distance between the transmitter and the receiver as well as their radio physical locations. In Generalized Attack Detection (GADE) method, K-means clustering method is used to perform clustering analysis in RSS. An important consideration is how the RSS readings vary widely and cluster together. Over time, these RSS readings from the same physical location forms similar clusters in n-dimensional signal space. In case of a spoofing attack, both the victim and the attacker use the same ID to transmit data packets. Thus, spoofing detection is formulated as a statistical significance testing problem. Here the null hypothesis is μ0: normal or spoofing attack has not occurred [12]. In the significance testing method, a test statistic, T is used to evaluate whether the data that is observed, satisfies the null hypothesis condition or not.

- Spoofing Attack Prevention System: The proposed system introduces an intermediate node that lies between the users and the server. Once the attack has been detected by the Generalized Attack Detection module, the intermediate node is made aware of the situation. The intermediate node filters out the data requests in the way that while it may still receive requests from the attackers but it does not forward it to the sever [13]. This prevents the attacker from gaining access to the data from the server. This process is illustrated in the diagram below.
- Intrusion Detection and Prevention System: Essentially, intrusion detection is a set of actions that that determine and report illegitimate activities in wireless sensor networks. Communication amongst the wireless sensors in a network is done using wireless transceivers. IDPS has the ability to identify network intrusions by collecting and analyzing data. Wireless IDPS can monitor the activities of the system as well as users, identify previously accounted attack patterns and report the same to a source node to avoid losing an important event. The proposed system introduces a Control Authenticator that distributes both public and private keys to all the nodes in a cluster. Based on the public key, the IDPS monitors the activities of all nodes in a cluster by tracking parameters such as transmission power and energy levels. When the source node, S starts sending the packets to the destination node, D the sender node checks for these exact same parameters using the private key that is shared only between the two nodes. If there is an anomaly in the values of transmission power calculated, an attack has occurred. The IDPS alerts the source node and all other nodes about the attack before eventually dropping the packet. The source node then re-routes the data packet to the destination node using the AOMDV routing protocol. This mechanism is highly effective as it reduces packet drop and increases the throughput. Moreover, two types of detection techniques are used, namely signature detection and anomaly detection. In case of signature detection, the IDPS compares the current activity of the nodes with stored attack profiles and generates an alarm in case a discrepancy arises. In the case of anomaly detection, the IDPS compares the system's normal profile with the current activity. Modern IDPS technologies offer automation of tasks such as notifying the administrator in the case of attack detection, closing the malicious connection etc. However, it is important to monitor the IDPS logs regularly. The proposed algorithm creates an IDPS node with AOMDV as the routing protocol. The

IDPS node then checks the network configuration and capture load by finding any node in its radio range and ensuring that the next hop is not null following which it moves on to capturing all the information from the nodes. IDPS then creates a normal profile which contains data like the type of packet, time of sending and receiving the packet and establishes a threshold value based on the profile. The IDPS then infers that if in any case, the network load turns out to be greater than the threshold limit, an attack has occurred. In such a scenario, it blocks the packet sender node, much like RADAR [14].



.

Figure 2: Spoofing Attack Prevention System.

6. Performance and Result Analysis

A number of simulations were carried out in order to compare the performance of the proposed system with the existing system like DSR, DSDV, ADMOV, EAACK, EAB in a simulated environment created over Network Simulator 2 in Ubuntu 10.04

6.1. Resilience Comparison

Figure 3

Resilience is the capacity to provide an acceptable level of service even in the case of operational challenges. These can be anything from simple misconfiguration over large scale natural disasters to target attacks. In order to increase the resilience, these challenges have to be identified and mitigated. In the graph shown above, we compare the resilience performance of proposed intrusion detection algorithm against other existing intrusion detection algorithms like Dynamic Source Routing Protocol and EAACK Intrusion Detection System. According to the performance graphs of the proposed system, it shows a clear improvement over the existing [15] DSR protocol.

6.2. Number of detected intruder nodes versus simulation time

The number of intruders detected over time is one of the most important criteria over which an intrusion detection algorithm is judged. Here, the proposed system is being compared against various existing algorithms like DSB, DHC and DAB.

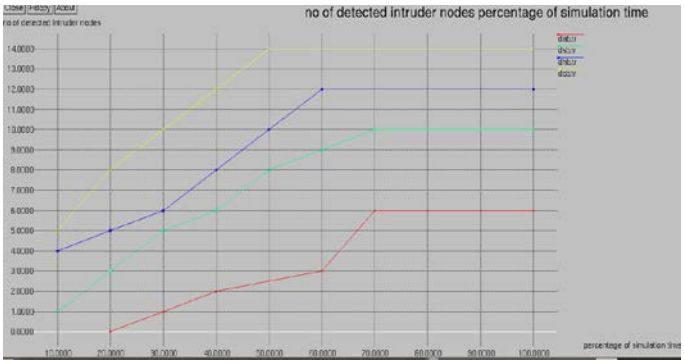


Figure 4

According to the graph, the performance of the proposed system is clearly superior as the rate of detection of attacker nodes of the proposed RSSI based intrusion detection system is better than existing systems.

6.3. Energy Consumption over the percentage of detected intruders

The amount of energy consumed is an indicator of the efficiency of the system.

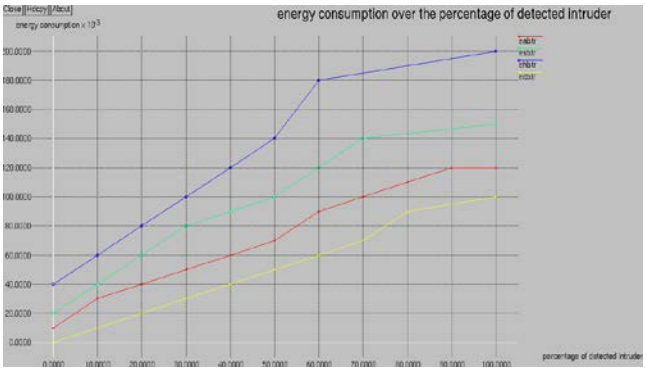


Figure 5

The graph compares the energy consumption of the proposed system with other existing algorithms like EAB, ESB and CHB and clearly indicates an improvement over them.

7. Conclusion

Wireless sensor networks are a highly effective and widely used means of communication. At its present state however, it is vulnerable to a lot of malicious attacks. The system needs to be made more robust in order to prevent loss of data and maintain optimal network performance. The proposed approach tries to introduce the concept of an Intrusion Detection System that can facilitate this task without adding any additional costs or requiring any type of modification to the existing wireless network. The results obtained are highly encouraging and can be easily visualized using tools such as Network Simulator. The future also holds various challenges with adversaries launching new types of attacks in order to gain illegitimate advantage. It is imperative then to be able to introduce other such concepts like the one based on RSS here, whose data is hard to falsify and cannot be easily manipulated by these attackers.

References

[1] Jie Yang, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe and Jerry Cheng. (2013). Detection and Localization of Multiple Spoofing Attackers in Wireless Networks. IEEE. 24 (1), p44-58

[2] M. Bohge and W. Trappe, “An Authentication Framework for Hierarchical Ad Hoc Sensor Networks,” Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

[3] A. Wool, “Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation,” ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

[4] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Detecting and Localizing Wireless Spoofing Attacks” Proc. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 2014.

[5] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, “Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,” Proc. IEEE Int’l Conf. Comm. (ICC), pp. 4646-4651,June 2007.

[6] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless Device Identification with Radiometric Signatures,” Proc. 14th ACM Int’l Conf. Mobile Computing and Networking, pp. 116-127, 2008.

[7] Q. Li and W. Trappe, “Relationship-Based Detection of Spoofing Related Anomalous Traffic in Ad Hoc Networks,” Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. And Networks (SECON), 2006.

[8] F. Guo and T. Chiueh, “Sequence Number-Based MAC Address Spoof Detection,” Proc. Eighth

Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.

[9] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 21372145, 2008.

[10] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," Proc. IEEE INFOCOM, Apr. 2008.

[11] D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[12] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, "A Practical Approach to Landmark Deployment for Indoor Localization," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Sept. 2006.

[13] E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int' Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

[14] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE INFOCOM, 2000.

[15] P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.