SPOOFING ATTACK - A THREAT IN WIRELESS SENSOR NETWORKS

Prasuna Kotturu[1] and Ch. Ramesh[2]

1. Final Year M.Tech, Department of CSE, Aditya Institute of Technology & Management, Tekkali, Srikakulam Andhra Pradesh.
2. Professor, Department of CSE, Aditya Institute of Technology & Management, Tekkali, Srikakulam Andhra Pradesh.

Abstract: There has been a growing interest in Wireless Sensor Networks (WSN). Recent advancements in the field of sensing, computing and communications have attracted research efforts and huge investments from various quarters in the field of WSN. Also sensing networks will reveal previously unobserved phenomena. The various areas where major research activities going on in the field of WSN are deployment, localization, synchronization, data aggregation, dissemination, database querying, architecture, middleware, security, designing less power consuming devices, abstractions and higher level algorithms for sensor specific issues. This paper provides an overview of ongoing research activities, various design issues involved and possible solutions in corporation these issues. This paper provides a cursory look at each and every topic in WSN and our main aim is to introduce a newbie to the field of WSN and make him understand the various to pictures of interest available for research. Now a day's Wireless spoofing attacks are very easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. This paper proposes to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis determination.

Keywords: Network Analysis, Spoofing Attack, Spoofing Detection, Localization, Wireless Network

Introduction

In wireless network it is very difficult to identify multiple spoofing attacks because wireless network has openness in nature and each and every node have their own node identity which is very essential to recognize and differentiate one node from other node. As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is very easy for an attacker to purchase a low price wireless device and can use these commonly available platforms to launch various type of wireless spoofing attack. There are different types of attacks which can be performed by attackers, among this attacks identity-based attacks are easy to launch and cause significant damage to network performance. Therefore, it is important to detect the presence of spoofing attackers, determine the number of attackers and to localize multiple adversaries ant eliminate them. The traditional approach to address spoofing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational poor associated with distributing, and maintaining cryptographic keys. Due to the limited, poor and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network. In this paper, I take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, I propose a scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) and a physical property associate with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Using spatial information to address spoofing attackers has the unique power to not only identify the presence of these attackers but also localize adversaries. It does not require additional cost or modification to wireless device to identify spoofing attacks. In this I proposed to use a general attack detection model (GADE) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis and an integrated detection and localization system (IDOL) which can detect both attackers as well as position of multiple attackers even when the attackers vary their power level. The scope of this paper is to detect spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries If an intruder comes during transaction, then server discover and localize that specific system. So that the data transmitted by the sender can be receive only by authenticated receiver not by the attacker who masquerades as the same identity of original node and to eliminate the attack to make data transmission secure. In the proposed system I proposed to use a generalized attack detection model (GADE) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods grounded on RSS based spatial correlations among normal devices and adversaries; and an integrated detection and localization system (IDOL) that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. In GADE, the Partitioning around Medoids (PAM) cluster analysis method is used to perform attack detection. After that I formulate the problem of determining the number of attackers as a multiclass detection problem and then I applied cluster based methods to determine the number of attackers. To improve the accuracy of determining the number of attackers a mechanism called SILENCE, when the training data are available, Support Vector Machines (SVM) method is used to further improve the accuracy of determining the number of attackers. Moreover, we developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. By this method it is possible to detect spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries without causing overhead in wireless network.

Preliminaries:

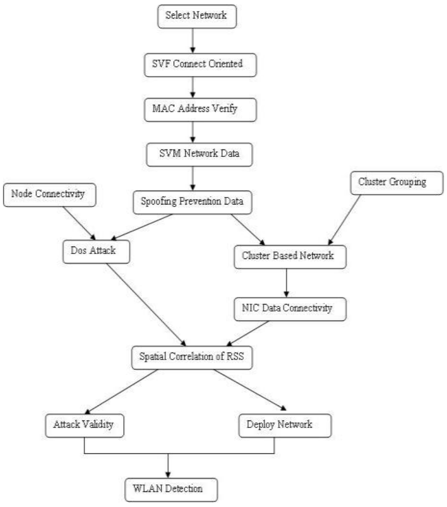
The main contributions of the work are:
1) GADE: a generalized attack detection model (GADE) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods grounded on RSS-based spatial correlations among normal devices and adversaries.
2) IDOL: an integrated detection and localization

system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels.

Generalized Attack Detection Model: In GADE, the Partitioning around Medoids (PAM) cluster analysis method is used to perform attack detection. We formulate the problem of determining the number of attackers as a multiclass detection problem. We then applied cluster-based methods to determine the number of attacker

Localization of Attackers: Identify the positions of multiple adversaries even when the adversaries vary their transmission power levels. The main contribution of the paper is organized are as follows:

- To effectively detect the presence of spoofing attack
- To count the number of attackers
- To identify the location of multiple adversaries in the network
- To provide solution to identify adversaries in the network where in there is no additional cost or modification to the wireless devices themselves
- To avoid authentication key management
- To avoid overhead
- To develop a mechanism where in there is low false positive rate



Real Vulnerabilities and Practical Solutions: The convenience of 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial and military sectors. However, this use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11's basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated. In fact, it has been suggested that 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management and media access protocols This paper provides an experimental analysis of such 802.11-specific attacks their practicality, their efficacy and potential low-overhead implementation changes to mitigate the underlying vulnerabilities.

We describe possible denial of service attacks to infrastructure wireless 802.11 networks. To carry out such attacks only commodity hardware and software components are required. The results show that serious vulnerabilities exist in different access points and that a single malicious station can easily hinder any legitimate communication within a basic service set.

Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to asquerade as a septic client or to create multiple illegitimate identities. For example, several link-layer services in IEEE 802.11 networks have been shown to be vulnerable to such attacks even when 802.11i/1X and other security mechanisms are deployed. In this paper we show that a transmitting device can be robustly indentured by its signal print, a topple of signal strength values reported by access points acting as sensors. We show that, deferent from MAC addresses or other packet contents, attackers do not have as much control regarding the signal prints they produce. Moreover, using measurements in a tested network, we demonstrate that signal prints are strongly correlated with the physical location of clients, with similar values found mostly in close proximity. By tagging suspicious packets with their corresponding signal prints, the network is able to robustly identify each transmitter independently of packet contents, allowing detection of large class of identity-based attacks with high probability.

Wireless networks are vulnerable to spoofing attacks, which allows for many other forms of attacks on the networks. Although the identity of a node can be verified through cryptographic authentication, authentication is not always possible because it requires key management and additional infrastructural overhead. In this paper we propose a method for both detecting spoofing attacks, as well as locating the positions of adversaries performing the attacks. We first propose an attack detector for wireless spoofing that utilizes K-means cluster analysis. Next, we describe how we integrated our attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. We then show that the positions of the attackers can be localized using either area-based or point-based localization algorithms with the same relative errors as in the normal case. We have evaluated our methods through experimentation using both an 802.11 (WiFi) network as well as an ZigBee network. Our results show that it is possible to detect wireless spoofing with both a high detection rate and a low false positive rate, thereby providing strong evidence of the effectiveness of the K-means spoofing detector as well as the attack localizer

The flexibility and openness of wireless networks enables an adversary to masquerade as other devices easily. Identity-based spoofing attacks are serious network threats as they can facilitate a variety of advanced attacks to undermine the normal operation of networks. However, the existing mechanisms can only detect spoofing attacks when the victim node and the spoofing node are static. In this paper, we propose a method for detecting spoofing attacks in the mobile wireless environment that is when wireless devices, such as the victim node and/or the spoofing node are moving. We develop the DEMOTE system, which exploits Received Signal Strength (RSS) traces collected over time and achieves an optimal threshold to partition the RSS traces into classes for attack detection. Fur ther, our novel algorithm alignment prediction (ALP), when without the knowledge of spatial constraint of the wireless nodes, utilizes temporal constraints to predict the best RSS alignment of partitioned RSS classes for RSS trace reconstruction over time. Our approach does not require any changes or cooperation from wireless devices other than packet transmissions. Through experiments from an office building environment, we show that DEMOTE achieves accurate attack detection both in signal space as well as in physical space using localization and is generic across different technologies.

Hierarchical architectures are more and more widely adopted for organizing wireless sensor networks. In such architectures, middle-tier nodes take important roles, and preventing a malicious node from impersonating a middle - tier node and injecting falsified messages becomes critical. In this paper, we propose an energy efficient, distributed scheme to secure the multicast messages from the middle-tier nodes. Our scheme does not require a priori knowledge about the hierarchical relation between middle-tier nodes and lowest-tier nodes, and is adaptive to changes of this relation. Extensive simulations are conducted to evaluate our scheme, and the results show that the scheme is energy efficient.

Wireless LAN standard has been designed with very limited key management capabilities, using up to 4 static, long term, keys, shared by all the stations on the LAN. This design makes it quite difficult to fully revoke access from previously-authorized hosts. A host is fully revoked when it can no longer eavesdrop and decrypt traffic generated by other hosts on the wireless LAN. This paper proposes WEP ∗, a right weight solution to the host-revocation problem. The key management in WEP∗ is in the style of pay-tv systems: The Access Point periodically generates new keys, and these keys are transferred to the hosts at authentication time. The fact that the keys are only valid for one re-key period makes host revocation possible, and scalable: A revoked host will simply not receive the new keys. Clearly, WEP∗ is not an ideal solution, and does not address all the security problems that IEEE 802.11 suffers from. However, what makes WEP∗ worthwhile is that it is 100% compatible with the existing standard. And, unlike other solutions, WEP∗ does not rely on external authentication servers. Therefore, WEP∗ is suitable for use even in the most basic IEEE 802.11 LAN configurations, such as those deployed in small or home offices. A WEP∗ prototype has been partially implemented using free, open - source tools.

Generalized Attack Detection Model (GADE): It can both detect spoofing attacks as well as determine the number of adversaries using Cluster analysis. In GADE, the Partitioning Around Medoids (PAM) cluster analysis method is used to perform attack detection and then applied cluster-based methods to determine the number of attacker.

PAM: This method is a popular iterative descent clustering algorithm. Compared to the popular K-means method, the PAM method is more robust in the presence of noise and outliers. Spoofing attack detection is performed using Cluster Analysis. As the wireless network is deployed as clusters, the attackers are identified in each and every cluster separately. Consider the wireless nodes are composed of several clusters of ordinary Nodes. The PAM algorithm partitioned a dataset of ‘n’ objects into a number of clusters (‘k’), where both the dataset and the number k is an input of the algorithm. This algorithm works with a matrix of dissimilarity, where its goal is to minimize the overall dissimilarity between the represents of each cluster and its members.it shows how Spoofing attacks are detected by same location id. Attacker gets the ID of normal node and makes use of the same to send packets to Destination node.

In this section we describe our approach in solving the problem of detection and localization of multiple spoofing attacks. Received signal strength is widely used for finding or estimating the location of a node from which signals are received. Based on the signal strength it is achieved. However, it might not be as accurate as expected. To overcome this problem in RSS is used along with spatial correlation. The RSS readings provide details about spatial correlations. This will help in finding exact location of the mobile device. The detection and localization of spooling attackers is achieved using RSS and its spatial correlations. More details about the solution can be found in. In this paper we built a prototype application that demonstrates the concept of detection and localization of multiple spoofing attackers. The application was built using Java platform. The nodes are built as graphical programs that simulate the functionality of wireless nodes. The application runs in networking environment. The application is basically a network application where multiple wireless nodes can run and there are common communication scenarios among the nodes. However, we built an attack model as well to demonstrate the detection and localization of multiple spoofing attackers. With attack model, the application is able to demonstrate the proof of concept.

Experimental Results: The environment used for experiments is multiple PC switch 2 GB RAM and core 2 dual processor running in a network. In each PC a graphical program runs which simulates as a wireless node. The nodes running different machines can communicate with each other. The general communication characteristics are provided in the network application besides the simulation of attack model. The application supports the selection of number of nodes in the network and generates the nodes as follows besides having a graphical program for each node. As can be seen in Figure 3, the packet transmission process in the normal scenario is demonstrated RSS vector is generated and it is used for computing the required values in order to perform detection and localization of attackers. the cluster analysis is made for understanding the nodes, their positions and the cluster to which they belong. These cluster dynamics are further used later for detection and localization will takes place in the application is able to demonstrates multiple spoofing attacks and able to detect spoofing attacks, the application is able to detect the number of attackers. The attackers and other details are computed. the attackers are localized. The number of attackers involved in spoofing attack and their location is found. it is evident that the node localization dynamics are visualized. The horizontal axis takes nodes, x and y dimensions while the vertical access presents accuracy.

Attack Detection Using Cluster Analysis: Distributed Denial of Service (DDoS) attacks generate enormous packets by a large number of agents and can easily exhaust the computing and communication resources of a victim within a short period of time. In this paper, we propose a method for proactive detection of DDoS attack by exploiting its architecture which consists of the selection of handlers and agents, the communication and compromise, and attack. We look into the procedures of DDoS attack and then select variables based on these features. After that, we perform cluster analysis for proactive detection of the attack. We experiment with 2000 DARPA Intrusion Detection Scenario Specific Data Set in order to evaluate our method. The results show that each phase of the attack scenario is partitioned well and we can detect precursors of DDoS attack as well as the attack itself.

Detection using Clustering Data Mining:

Firewall device may not detect and prevent many types of DDoS attack passing through the network traffic because of its security weakness. In DDoS attacking time, attacker may carry out the attack packet with genuine packets which cause more harmful to the victim and difficulty for firewall in detection for this type of attack. Moreover, the attacker uses spoofed IP causing the tracing process more difficult DoS tack can be implemented through many layers of TCP/IP layers. UDP/ICMP flooding attacks send a large number of UDP/ICMP packets to the victim which limits the communication link and make overall congestions. Web server may attack with HTTP GET flood attack which causes Denial of Service (DoS) attack by repeatedly request to download the web page On the other hand, many researchers adopted clustering with statistical model and machine learning to limit the damaging of DDoS attacks but in a limited scale [9-10]. Data mining clustering techniques comes to overcome the limitation in statistical models and other techniques that used to detect and prevent the DDoS attacks. For instance, statistical models limit the performance of communication bandwidth due to overhead of sampling packets in real-time. In case of DDoS attack, modelling and estimation network traffic is difficult because the network traffic has linear and burst characteristics [11]. In general, it is very hard to obtain anomaly detection in a real attack as in the case of DDoS attack because most works for DDoS attack use flows realized in laboratories by means of DDoS traffic generator tools [3]. In this paper, centroid-based rules method is firstly used one of the unsupervised data mining clustering method and it is secondly used the supervised proactive rules. This method is designed and implemented to effectively analyse and detect a DDoS real-world attack from CAIDA data set. Centroid-based rule clustering is approached as one of the hybrid machine learning techniques as follow. CAIDA data sets split into training and testing data after the pre-processing phase. Splitting the data set into training and testing phases is coming to create the rules profile, which used later in model Performance. In the forming of cluster phase, we find centroids which represent a data point center for each particular cluster. Given a set of E independent data items {t1, t2, t3, ...tn} and specify the number of clusters {c}, the outputs of cluster analysis method are {C} clusters with theirs centroids. In the rules phase, specify two sets of data points {m1, m2) and (n1, n2) that represent the max-min data points respectively in each cluster in on-line mining. Centroid-based rule are applied to extract max-min data points after the forming of clusters phase. In the testing phase, the rules are used later to test any data point for attack possibility. Centroid based method is very efficient during the training phase and consequently the rules method as they are based on the number of centroids. A little CPU consumption and space complexity is involved in this hybrid method by testing each testing data point with max-min rules to differentiate the legitimate and malicious traffic.

Network Traffic and Feature Selection: The DDoS attacks and normal traffic are collected from the variety of CAIDA datasets as described in the section 3. Two million (2,000,000) network packets are selected from both data sets for attack and normal traffic. A proactive system based on centroid-based rules only works on TCP/IP header information of the TCP/IP packets. Since the payload is removed from “The CAIDA "DDoS Attack 2007 Dataset” and “The CAIDA Anonymized Internet Traces 2008 Dataset”, the most important features (attributes) are described

Data Transformation and Standardization: A major step in traffic pre-processing is data transformation. Information theory is a crucial step to convert the data from one format to another format. Shannon's entropy method is selected in this pre-processing step. The entropy method works with categorical data and scales well to extremely large data sets [22-23]. Consider a network traffic having n independent packets, each with probability of Pi, the entropy H algorithm is defined for data transformation and standardization. Finally, max-min normalization method, which performs linear transforming on the original traffic data, is selected for data normalization. Which illustrated data transformation and standardization pseudo-code algorithm?

Evaluation Procedure : Wireless Sensor Networks (WSNs) use tiny, inexpensive sensor nodes with several distinguishing characteristics they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific monitoring and sensing functions. Several such wireless sensors in a region self-organize and form a WSN. Information based on sensed data can be used in agriculture and livestock, assisted driving or even in providing security at home or in public places. A key requirement from both the technological and commercial point of view is to provide adequate security capabilities. Fulfilling privacy and security requirements in an appropriate architecture for WSNs offering pervasive services is essential for user acceptance. Five key features need to be considered when developing WSN solutions: scalability, security, reliability, self-healing and robustness. The required strength of each of these features depends on the application in question. Current trend of networked embedded computing technology is to involve humans as part of the sensing, data collecting and computing. In this way, public and professional users are able to gather, analyze and share local information to form advanced knowledge about the surrounding physical or social world. Instead of dedicated infrastructure or special designed networks, it is more convenient and efficient to collect commonly interested information and knowledge through wireless sensor networks. The emerging applications with wireless sensor networks involve human as a part of sensing, data collecting, and computing. These applications announce the advent of a new era of ubiquitous computing and communication.

Applications:

A wide range of applications of wireless sensor networks is anticipated in the following areas: public/community health monitoring, vehicular and transportation control, urban infrastructure management/planning, etc. Let’s consider an advanced metering system as an example to explain our proposed protocols, and design simulation scenarios. Utility companies are expecting millions of the wireless meters in the coming years. Besides automatic reading, the great potential of advanced metering systems is the ability to implement innovative rate policies. The wireless metering systems can provide real-time utility consumption that will help customers decide when they should increase their electricity usage to take advantage of cheaper power prices during low-demand periods or reduce usage when demand rises. Advanced metering this by collecting power consumption information hourly or even in smaller intervals. The major characteristics of civilian wireless sensor networks are summarized as follows.

Data Aggregation: The dominant traffic is data traffic. Usually people desire to get high level statistics rather than to learn individual behavior to capture the major feature of the surrounding systems. For example, in advanced metering systems, in order to determine pricing policies, real-time aggregated utility consumption information indicates whether or not it is the peak time of utility usage. For this purpose, utility consumption of individual households is not important. This means data aggregation is an important function in wireless sensor networks. On the other hand, information collection in such a system with fine granularity and over a large population will introduce a huge bandwidth demand, so it requires efficient means to get the aggregated statistics of utility consumptions. Hence, in network aggregation is needed.

Resource Constraints: Advances in miniaturization and nanotechnology enable us to reduce the size and cost of embedded devices for sensing, computation and wireless communication in physical world. However, small-size and low-cost devices usually have limited power, computation and storage. Also, the shared medium nature and interferences of multi-hop wireless communications imply limited bandwidth among low-power embedded devices.

Privacy & Integrity Concerns: Privacy and integrity are major concerns in collection of utility consumption information. If your neighbors or people around your house know the utility consumption information of your household, they can easily infer when you are on vacation, when you go to work, when you are taking shower, etc. On the other hand, integrity of the aggregated statistics about the utility consumption is a prerequisite to ensure correct pricing, appropriate load balancing, and in general avoid chaos in advanced metering systems.

Large Scale: The proliferation of embedded devices and the advances of the networked embedded systems provide means to gather data on large scales. In the advanced metering example, millions of advance meters are involved in a certain area. We anticipate that large-scale, on-line data collection and processing paradigms will make great impact on both physical systems and social behaviors. Hence, scalability is one of the major design concerns.

Challenges : Providing efficient data aggregation while preserving data privacy and integrity is a challenging problem in wireless sensor networks due to the following factors:

1. Trust management in WSN is very challenging. Users in the wireless sensor networks can be very curious to learn others' private information, and the communication is over public accessible wireless links, hence the data collection is vulnerable to attacks which threaten the privacy. Without proper protection of privacy, the communication of privacy-sensitive data over civilian wireless sensor networks is considered impractical.

2. During in-network aggregation, adversaries can easily alter the intermediate aggregation result and make the final aggregation result deviate from the true value greatly. Without protection of data integrity, the data aggregation result is not trustworthy.

3. Data collection over wireless sensor networks does not rely on dedicated infrastructure. In many cases, the number of nodes answering a

query is unknown before the data aggregation is conducted.

4. Resource limited portable devices cannot afford heavy computation and communication load

5. The requirement on accuracy of information collection (i.e., aggregated result) makes the existing randomized privacy-preserving algorithms not suitable. Besides the above mentioned factors, it is very challenging to protect privacy and integrity of data aggregation simultaneously, because usually privacy - preserving schemes disable traffic peer monitoring mechanisms, which reduces the availability of information in a neighborhood to verify data integrity

Attack Detection Using Cluster Analysis:

The RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection. It also showed that the RSS readings from a wireless node may fluctuate and should cluster together. In particular, the RSS readings over time from the same physical location will belong to the same cluster points in the n-dimensional signal space, while the RSS readings from different locations over time should form different clusters in signal space. Which presents RSS reading vectors of three landmarks (i.e., n = 3) from two different physical locations. Under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings of that ID is the mixture readings measured from each individual node (i.e., spoofing node or victim node).Thus formulate spoofing detection as a statistical significance testing problem, where the null hypothesis is H0 : normal (no spoofing attack):In significance testing, a test statistic Tis used to evaluate whether observed data belong to the null-hypothesis or not.

Spoofing Attacks:

Spoofing attacks are easy to launch and can cause damage to the performance of a network. In an 802.11 network, it is easy for an attacker to collect a MAC address during passive monitoring and then attacker modify the MAC address by simply issuing an If configuring command to masquerade as another device. In the proposed system the frames like data, management, control are said to be protected. In the existing security techniques like Wired Equivalent Privacy, WiFi Protected Access, or 802.11i, such techniques can only protect the data frames, an attacker can spoof management or control frames to cause impact on networks.

Attack Detection:

In the attack detection instead of cryptographic based method, My work is new because none of the existing work can determine the number of attackers when there are more than one enemies masquerading as the same identity. The spatial correlation of RSS is used to detect the attack. The cluster based mechanism is used to detect the number of attackers. This mechanism is said to be improved by the support vector machine. That is the SVM is used to improve the accuracy of determining the number of attackers.

Localization:

The proposed approach can correctly localize more than one enemies even the transmission power levels of the attackers varies. Algorithm used for a localization are area based probability and RADAR gridded algorithms. Localization estimation using RSS which are about 15 feet. When the nodes are less than 15 feet apart, they have a high likelihood of generating similar RSS readings, and thus the spoofing detection rate falls below 90 percent, but still greater than 70 percent. When spoof moves closer to the attacker also increases the probability to expose itself, now the detection rate goes to 100 percent. When the spoofing node is about 45-50 feet away from the original node. The detection rate is said to be lesser.

The Evolution of an Experimental Wireless Sensor Network : Self organizing mobile Sensor and data networks (SomSed) is a research field at the Hamburg University of Technology. While the cooperation among the professors of the institutes is common, doing research in cooperation between under- graduates and Ph.D. students of different institutes is rare. Institutes work together in a matrix like organization structure on topics concerning wireless sensor networks. In doing so, the institutes can concentrate on their core competences concerning this research field. The unique collaboration of several institutes forms a broad basis for research. The Ph.D. students branch of Soused focuses on their own special research topics and implemented a wireless sensor network on the campus of the Hamburg University of Technology. The cooperation on undergraduate and Ph.D. student level also profits from this approach and leads to additional synergy effects and knowledge transfer between the collaborating institutes. The institutes themselves use the knowledge gained in Soused. For example, experiences gained in Soused are used to build up sensor networks for cruise and container vessels, and doing feasibility studies of using 2.4GHz applications in these environments. Another approach is to investigate multi-coverage based broadcasting in order to increase reliability in a wireless sensor network, as presented in. In this approach an Integer Linear Program (ILP) has been applied to multimedia data transmission inside an aircraft passenger cabin. The solution provides compact routing and scheduling of the relaying nodes.

II. CAMPUSNET During the last year SomSed-Active developed and deployed an experimental wireless sensor network on the campus referred to as Campus Net. The Campus Net consists of 26 fixed nodes of type IRIS from the company Crossbow Technology [4]. The nodes are based on an ATmega1281 microprocessor with an integrated 2.4 GHz IEEE 802.15.4 radio transceiver. The nodes run the open source pirating system TinyOS version 2.x. Before the construction of the Campus Net started a series of open field measurements of connectivity and signal strength of the IRIS nodes have been carried out. The results of these measurements were used to find an adequate placement in terms of connectivity for the participating nodes. The placement of the nodes is shown in using small circles. The software for the Campus Net can be divided into three parts: The sensor node firmware, which is responsible for routing, tree construction, sensing, power management and data buffering, and the frontend and backend software. The backend software just persists incoming data from the sensor network into a database and is the initiator of regularly occurring tree constructions. The frontend software is used for analysis and visualization of the stored information. The routing mechanism and the frontend software are described in more detail in the following sections.

Conclusion

In this paper, we present a brief survey on threads on wireless sensor network, its characteristics and its types. Then we discussed about the security in sensor networks, security issues and various DoS attacks on different layers. Security is an important requirement and complicates enough to set up in different domains of WSN. We also discuss various dimensions of security (availability, integrity, confidentiality and authenticity) that are being directed by different physical attacks. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

References:

1. S. Georgi, C. Weyer, M. Stemick, C. Renner, F. Hackbarth, U. Pilz,J. Eichmann, T. Pilsak, H. Sauff, L. Torres, K.Dembowski, and F. Wagner, "Somsed: An interdisciplinary approach for developing wireless sensor networks," 7. GI/ITG KuVS Fachgesprach Drahtlose Sensornetze, Berlin,Germany, Tech. Rep. B 08-12, 2008.

2. T. Pilsak and J. ter Haseborg, "Emc feasibility study of the use of 2.4-ghz-wlan applications on bridges of cruise and container essels,"inElectromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium on , Detroit, MI, USA, Aug. 2008, pp. 1–6.

3. L. Torres and U. Killat, "Routing and scheduling for short-range wireless inflight multimedia networks," in Proceedings of the 2nd International Workshop on Aircraft System Technologies (AST 2009) , O. von Estorff and F. Thielecke, Eds. Hamburg, Germany: Shaker Verlag, Aachen,Mar. 2009, pp. 337–346.

4. C. Lange, "Energiegewinnung fur drahtlose Sensorknoten," Master's thesis, Hamburg University of Technology, Hamburg, Germany, Oct. 2008.

5. M. Stemick, A. Boah, and H. Rohling, "Over-the-air programming of wireless sensor nodes," 7. GI/ITG KuVS Fachgesprach DrahtloseSensornetze, Berlin, Germany, Tech. Rep. B 08-12, 2008.

6. Dittrich, D., Weaver, G., Dietrich, S., and Long, N. (2000) The 'mstream' Distributed Denial of Service attack tool. Technical re- port. University of Washington, Seatlle, USA,

7. http://stawashington.edu/dittrich/misc/mstream.analysis.txt.

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. F. Ferreri, M. Bernaschi, and L. Valcamonici "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," Proc. IEEE Wireless Comm. and Networking Conf., 2004.

10. D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signal prints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

11. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.

12. P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF- Based User Location andTracking System," Proc. IEEE INFOCOM, 2000.

13. 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

14. N. Cristianini and J. Shawe-Taylor, An Introduction to SupportVector Machines and Other Kernel-Based Learning Methods. Cam-bridge Univ. Press, 2000.

15. C.-C. Chang and C.-J. Lin, LIBSVM: A Library for Support Vector Machines, Software, http://www.csie.ntu.edu.tw/cjlin/libsvm,2001.

16. V. Franc and V. Hlava ´c, "Multi-Class Support Vector Machine,"Proc. Int'l Conf. Pattern Recognition (ICPR), vol. 16, pp. 236-239, 2002.

17. C. Hsu and C. Lin, "A Comparison of Methods for Multiclass Support Vector Machines," IEEE Trans. Neural Networks, vol. 13, no. 2, pp. 415-425, Mar. 2002.

18. D. Madigan, E. Elnahrawy, R. Martin,W. Ju, P. Krishnan, and A.S.Krishnakumar, "Bayesian Indoor Positioning Systems," Proc. IEEE, INFOCOM, pp. 324-331, Mar. 2005.

19. J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. USENIX Security Symp., pp. 15-28, 2003.

20. F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," Proc. IEEE,Wireless Comm. and Networking Conf., 2004.

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

22. 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.

23. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc.IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.

24. 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.

25. 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