SPOOFING ATTACK DETECTION AND LOCALIZATION IN WIRELESS SENSOR NETWORK: A REVIEW

P. KIRUTHIKA DEVI

Research Scholar
Department of Computer Science,
K.S.Rangasamy College of Arts and Science,
Tiruchengode-637215, India
Email: *kirthi.bala90@gmail.com*

Dr. R. MANAVALAN

Department of Computer Applications,
K.S.Rangasamy College of Arts and Science,
Tiruchengode-637215, India
Email: *manavalan_r@rediffmail.com*

Abstract---Spoofing attack is an identity based attack through which a malicious user can spoof the MAC address of a node to create multiple illegitimate identities that highly affect the performance of wireless sensor network. The identification of spoofers and localization of the same is a challenging task in wireless sensor network. This paper presents expository survey of various spoofing attack detection techniques in wireless sensor network.

Keywords: Wireless network security, spoofing attack, attack detection, localization.

I. INTRODUCTION

Device identity is perhaps one of the most challenging problems in any network for security. Localizing node is necessary for many higher level network functions such as tracking, monitoring and geometric-based routing and also used in broad area. It is easy to attack MAC addresses in IEEE 802.11 wireless network using publicly available tools. It is possible to implement many 802.11 attacks easily with the purchase of low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with a little effort.

Spoofing attacks can further create a variety of traffic injection attacks [51], [8] such as attacks on access control lists, rogue access point attacks, and eventually Denial-of- Service (DoS) attacks. Moreover, in a large-scale network, multiple adversaries may masquerade the same identity of the node and launch malicious attacks such as network resource utilization attack and DoS. Therefore, most of the approaches are introduced so for to prevent from spoofing attacks in wireless sensor network. It is important to detect the presence of spoofer in wireless network, determine the number of attackers, and finding the location of multiple adversaries and defeat them.

The presence of spoofing attack detection, count the number of attackers, identify the location of multiple adversaries in the network are challenging task in wireless sensor network. These problems are addressed by various authors by introducing different approaches. A number of traditional approaches are used in authentication application to address the problem of spoofing attacks [52]. However, authentication requires additional infrastructure and computational power associated with distributing, and maintaining cryptographic keys. A study on spoofing attack on wireless sensor network is presented in section II. The rest of the paper is organized as follows: section II provides a brief survey of spoofing attack in wireless sensor network. Finally the issues of detection and localization of spoofing attack are discussed in section III and present the conclusion in section IV.

II. SPOOFING ATTACK ON WIRELESS SENSOR NETWORK: A REVIEW

In 2000 Kihong Park and Heejo Lee [1] proposed the concept of probabilistic packet marking (PPM) for tracing the source (i.e.) origin of DoS attack. The effectiveness of PPM is evaluated in a mini max adversarial context where the attackers spoof the marking field to make maximum confusion at the source node. The attackers have the ability to affect the nodes that is reduced by choosing the suitable marking probability. For single source attack, PPM is effective for localizing the attacker’s origin. The result showed that PPM approach effectively localizes the spoofing in order to improve the performance of network. **.(“On the Effectiveness of Probabilistic Packet Marking for IP Trace back Under Denial of Service Attack”)**

In 2000, Balachander Krishnamurthy and Jia Wang [2] proposed a “Network-Aware" method, to identify client clusters by using the prefixes and netmasks information which is extracted from BGP (Border Gateway Protocol) routing table. A self-correction and adaptation mechanism was also used to improve the applicability and accuracy of the initial cluster identification increased. The entire cluster identification process can be done in an automated fashion while moving from a server log to a set of interesting client clusters. The cluster information can be used in applications such as content distribution, caching, and network management. A useful byproduct is the identification of spiders and proxies among Web clients by examining the accessing patterns of corresponding client clusters. The result showed that the method is suitable to group more than 99.9% of the clients captured in a wide variety of server logs into clusters. **(“On network-aware clustering of Web clients”).**

In 2000, P. Bahl and V.N. Padmanabhan [3] proposed and demonstrated the method RADAR for identifying the location of attacker in wireless sensor network. The method is developed based on the physical location of the authorized as well as unauthorized users. The RADAR has all information about the authorized users in the client server communication. If any unauthorized user is accessing the data then the corresponding information will be stored in RADAR. So, it is easy to identifying the attacker. **(“RADAR: An in- Building RF- Based User Location and Tracking System,”)**

In 2001, Maurizio A. Spirito [4] proposed the multilateration techniques that process absolute and/or relative distance measurements. Based on this scheme, a general measure of accuracy has been derived and analyzed. The method helps to determine the positioning accuracy, measurement accuracy, and geometric conditioning of the problem. Formula used to calculate the location accuracy is GDoP (Geometric Dilution of Precision) by combining the areas of parallelograms determined by the reciprocal location of MS (Mobile Station) and MBTSs (Multiple Base Transceiver Stations). The result showed that the technique provides the better location accuracy in mobile communication network. **(“On the Accuracy of Cellular Mobile Station Location Estimation”).**

IN 2002, C. Hsu and C. Lin [5] proposed the concept of ‘Support Vector Machine’ which is originally designed for binary classification and also used to solve multiclass problems. To solve multiclass problems, two all-together methods are designed for decomposition and compared with three binary classifiers: one-against-one, one-against-all and Directed Acyclic Graph (DAG). The result showed that the “one-against-one” and DAG methods are more suitable for solving multiclass problem than the other **(“A Comparison of Methods for Multiclass Support Vector Machines”).**

In 2002, T.Roos et al., [6] proposed the three different machine learning approaches namely Non-Probabilistic Nearest Neighbor method and two probabilistic approaches (i.e) Kernel, Histogram methods for solving the location estimation problem. The location estimation is considered as a machine learning problem in which the task is modeled to find how the signal strengths are distributed in different geographical areas based on a sample of measurements collected at several known locations. The probabilistic methods were found to be relatively robust with respect to the number of base stations used, the amount of calibration data collected, and the length of the history used in the location estimation. The result showed that the two probabilistic methods produced slightly better result than the Nearest Neighbor method**. (A probabilistic approach to WLAN user location estimation”)**

` In 2002, Daniel B. Faria and David R. Cheriton [7] proposed the mobility-aware access control mechanism which is more suitable for both wireless and wired environments. The mechanism is composed of the SIAP (Secure Internet Access Protocol) and SLAP (Secure Link Access Protocol) protocols that solves the problem by merging essential services in a secure way. By merging authentication and IP address assignment, SIAP avoids the effective of DoS attacks effectively against DHCP (Dynamic Host Configuration Protocol) servers. Shared keys are also used in SLAP protocol for handling multicast frames based attacks to disable them. The results showed that the proposed protocols are efficient enough to secure 802.11b network. **(“DoS and Authentication in Wireless Public Access Networks”).**

In the year of 2003, Bellardo and S. Savage [8] conducted an experimental analysis for identification of the attacks by using efficacy and potential low-overhead implementation to mitigate the underlying vulnerabilities. The authors suggested some steps to identify the attack and remove the same. The communication between client and AP (Access Point) is established by using authentication request and association request. During this communication, some attacker may access IP address. At the time of data sending the deauthentication message may send to the AP, and then AP again sends the same to client. The attacker can be identified and analyzed using potential stopgap countermeasures. The result showed that the mechanism effectively identify the DoS attacks. **(“802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions”)**

In 2003, Mathias Bohge and Wade Trappe [9] proposed a framework, called TESLA certificate, for the scalability problems in hierarchical ad hoc sensor networks. The proposed framework authenticates incoming nodes, maintains trust relationship during topology changes and provides data origin authentication for Ad Hoc sensor network. The weak nodes are not involved in the creation or validation of public key signatures. The result showed that the security certificate provides more secure, adaptable and scalable for Ad Hoc sensor networks. **("An Authentication Framework for Hierarchical Ad Hoc Sensor Networks").**

Pradeep Kyasanur and Nitin H. Vaidya [10] proposed modified IEEE 802.11 MAC protocol and correction scheme in 2003. The method use distributed contention resolution mechanisms for sharing the wireless channel. Handling of MAC layer's misbehavior is important for ensuring a reasonable throughput for share well behaved nodes. The proposed protocol easily detects the misbehavior nodes. The correction scheme is very effective in restricting the throughput of selfish nodes. The result showed that the scheme accurately predict misbehavior nodes. **("Detection and Handling of MAC Layer Misbehavior in Wireless Networks").**

In 2003, Ping Tao et al., [11] proposed a technique Traditional localization for increasing robustness. Malicious nodes can easily violate the assumptions by modulating their transmission power of each packet. The mechanism helps for locating mobile devices in an indoor environment; even if the nodes are malicious. The techniques sacrifice some amount of accuracy in the ideal case of localizing cooperative nodes where as it maintains robustness while facing a variety of model errors, including malicious nodes, nodes with different hardware. The result showed that the mechanism provides better localization accuracy of the system. **("Wireless LAN Location-Sensing for Security Applications").**

In 2003, Hao Yang et al., [12] proposed a HOURS technique to achieve DoS resilience in an open service hierarchy. HOURS provides high degree of service accessibility for each surviving node with rich connectivity, making the connectivity highly unpredictable and recovering it when its normal operations are disrupted. HOURS preserves the original hierarchical structure, and augments it with hierarchical overlay networks. When certain nodes are under DoS attack, user queries are routed across the overlays to bypass the failed nodes and reach the destination. It works in concert with proactive solutions, such as server replication, that enhance the DoS resilience of individual nodes. The result showed that it creates multidefence against DoS attacks towards building a highly resilient open service hierarchy. **("HOURS: Achieving DoS Resilience in an Open Service Hierarchy").**

In 2003, Minho Sung and Jun Xu [13] presented a technique called IP-trace back-based Preferential Packet Filtering to filter out the majority of DDoS traffic and improving the overall throughput of the legitimate traffic. The proposed scheme collects the attacked packet information and uses such information to preferentially filter out packets that are more likely to come from attackers. The edges are infected by attackers and the legitimate client has the clean edges. The proposed scheme filters out the packets with the marks of infected edges and removes the DDoS traffic. Simulation results showed that the proposed technique can improve the throughput of legitimate traffic by three to seven times during DDoS attacks. **("IP Trace back-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks").**

In 2004, F. Ferreri et al., [14] described the number of possible Denial of-Service attacks on the 802.11 access networks. The communication is done between client and AP by sending the request and responses of authentication. De-authentication message is sent to both client and AP if attacker attacks during communication. To achieve this communication, the Finite State Machine (FSM) is used. To be safe from the attacks, the FSMs provide the three frames that are active when the attack is on progress. The first frame is 'probe request flood' that scans the network area. The second frame is 'authentication request flood' which also scans the network and gets the information about the authenticated users. The third frame 'association request flood' which identifies the illegal access in the network. The results showed that the extent of vulnerability to DoS attacks strongly depends on the firmware used by the APs. **("Access Points Vulnerabilities to Dos Attacks in 802.11 Networks")**

In 2004, J. Hall et al., [15] demonstrated an approach, which is incorporation of Radio Frequency Fingerprinting (RFF) and a wireless Intrusion Detection System (IDS). RFF uniquely identify a transceiver based on the transient portion of the generated signal. Moreover, the success rate of a wireless IDS is also improved by correlating several observations in time, using Bayesian filters. Simulation results showed that the RFF technique successfully address the intrusion detection problem in wireless network. **("Enhancing Intrusion Detection In Wireless Networks Using Radio Frequency Fingerprinting (Extended Abstract)").**

In the year of 2005, A.Wool [16] proposed Wired Equivalent Privacy (WEP) encryption technique which provides key management to address host-revocation problem. The IEEE 802.11 Wireless LAN standard has been designed with very limited key management capabilities and it makes quite difficult to fully revoke the access from previously authorized hosts. Using the technique, Access Point periodically generates new keys and transferred the same to the hosts at given authentication time. The fact is that the keys are only valid for one rekey period of making possible host revocation and scalable. A revoked host will not simply receive the new keys. WEP is quite simple, very efficient, as well as has no additional requirement beyond the AP and hosts. **(“Lightweight Key Management for IEEE 802.11 Wireless Lan With Key Refresh and Host Revocation”).**

Wu et al., [17] proposed a Secure and Efficient Key Management (SEKM) framework in 2005 to build a Public Key Infrastructure (PKI) by using a secret sharing approach and an underlying multicast server group. In SEKM, the cluster of server creates a Certification Authority (CA) view and provides certificate update service to all nodes and servers themselves. A ticket based scheme for efficient certificate service and efficient server cluster updating scheme are used in SEKM. It is noted that the coordination of server within the group is more efficient rather than the entire network during the secret share updating phase. The result showed that the server group provides certificate update service for all nodes including the servers themselves which are more efficient than the other. **(“Secure and Efficient Key Management in Mobile Ad Hoc Networks”).**

In 2005, Yang Xiao et al., [18] proposed two approaches to enhance security which are Keyed Message Authentication Code and Enhanced Authentication (WEP-KMAC-EA) and to enhance the WEP with Private IV and Session/Day Keys (WEP-PIV-SDK) to overcome some known vulnerabilities and thus to provide better data confidentiality and authentication. Key Management is partially solved since the system is not easily compromised despite the secret key remaining unchanged for a long time. Message Tampering is completely avoided from the use of Keyed Message Authentication mechanism. The result showed that the proposed enhancements provide better data confidentiality with some degree of computing cost. **(“Vulnerabilities and Security Enhancements for the IEEE 802.11 WLANs”).**

F. Guo and T. Chiueh [19] proposed an algorithm called Sequence Number-Based Spoof Detection algorithm in 2006 to detect the spoofed MAC address effectively without any changes in APs or STAs. By using the sequence number field in the IEEE 802.11 MAC header, all existing spoofing attacks can be detected without any false positive or negative. The false positive rate of the proposed algorithm is zero where as the false negative rate is closer to zero. The test results showed that the algorithm can tolerate STAs with abnormal sequence number evolution patterns without generating any false positives. Each spoofed frames will be detected if casual attackers don't exploit the false negative. **(“Sequence Number-Based MAC Address Spoof Detection”).**

In 2006, D. Faria and D. Cheriton [20] introduced the client and server communication for wireless network like Wi-Fi connection. The strength of each signal is calculated whenever the communication is held between client and server in wireless network. The value of each signal is closer to the specified range called as the ‘signal print value’ which totally depends on the physical location of the client. If the value of the signal print falls in same range then that signal is sent by the authenticated user or unauthenticated user. **(“Detecting Identity-Based Attacks in Wireless Networks Using Signal prints”)**

In 2006, Y.Chen et al., [21] proposed Linear Least Squares (LLS) and maxL-minE algorithm. The LLS algorithm is used for finding the localization error in the landmark. It also reflects the placement of landmarks as well as measurement errors at the landmarks. Further maxL−minE, algorithm is used for finding the optimal landmark placement to minimize the maximum localization error. The experimental results showed that the algorithms improve the localization performance of networks. **(“A Practical Approach to Landmark Deployment for Indoor Localization”)**

Kai Zeng et al., [22] proposed a Reciprocal Channel Variation-based Identification (RCVI) technique in 2006. Identity-Based Attacks (IBAs) are one of the most serious threats in wireless networks. The RCVI method is built based on RSS technique, to detect IBAs in mobile wireless networks. RCVI takes advantage of the location decorrelation, randomness, and reciprocity of the wireless fading channel to decide whether all the packets come from a single sender or more. If the packets are only coming from the genuine sender, then RSS variations are reported by the sender that should be correlated with the receiver’s observations. Otherwise, the correlation should be degraded and then an attack can be flagged. Results showed that RCVI achieved desirable performance under the tested scenarios and allows the user to tune the parameters to achieve strong security strengths. **(“Identity-Based Attack Detection in Mobile Wireless Networks”).**

In 2006, Fanglu Guo et al., [23] presented spoof detection strategies for protecting Domain Name System (DNS) servers from DoS attacks. These strategies create some form of cookies for a DNS server to check whether each incoming request is from the source node or from other. Each DNS requester needs to obtain a unique cookie from a ANS (Authoritative Name Server). Spoofed requests cannot present correct cookie, thus it can be detected. The result showed that it can deliver up to 80K requests/sec to legitimate users in the presence of DoS attacks at the rate of 250K requests/sec **(“Spoof Detection for Preventing DoS Attacks against DNS Servers”).**

In 2007, Yingying Chen et al., [24] proposed two approaches K-means cluster analysis and Area-based or Point-based Localization algorithms for wireless spoofing attack. The K-means is integrated as attack detector into a real-time indoor localization system, for localizing the positions of the attackers using either area-based or point-based localization algorithms. The results showed that it is possible to detect wireless spoofing in both a high detection rate and a low false positive rate. **("Detecting and Localizing Wireless Spoofing Attacks").**

In 2007, Xiao L and Trappe W [25] proposed a physical layer algorithm for enhancing authentication in a wireless in-built environment. The technique uses channel frequency response measurements and hypothesis testing to determine whether current and prior communication attempts are made by the same user. In this way, legitimate users can be reliably authenticated and false users can also be reliably detected. The result showed that the efficiency of the approach is in terms of static channel conditions. **("Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication")**

In 2007, Qing Li and Wade Trappe [26] presented a non cryptographic mechanism for detecting device spoofing on a wireless network. The method is complementary to authentication and can detect device spoofing with little or no dependency on cryptographic keys. The forge-resistant relationships associated with transmitted packets, and forge-resistant consistency checks allow other network entities to detect anomalous activity. The method uses sequence number field and temporary identifier fields for the evaluation according to a one-way function chain. **("Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationship").**

In 2007, Ruiliang Chen et al., [27] proposed two schemes; AD (Attack Diagnosis) and PAD (Parallel Attack Diagnosis) for DDoS countermeasures. Attack Diagnosis (AD), is an attack mitigation scheme that adopts a divide-and-conquer strategy. It is also called reactive defense mechanism that is activated by a victim host after an attack is detected. The victim host can trace back attack source and command an AD enabled router closer to the source for filtering the attack packets. An extension of AD called Parallel Attack Diagnosis (PAD) that is capable of throttling traffic coming from a large number of attackers simultaneously. The simulation result indicated that AD/PAD techniques that provide supports for incremental deployment, and incurs low false positives. **("A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks").**

In 2008, Y. Sheng et al., [28] proposed a spoofing detection approach based on Gaussian mixture models. The GMM is the mixture local statistics of a single AM, combining local results from AMs, and global multi-AM detection, respectively. The spoofing detection method is used for RSS profiling, and show how to use it to detect spoofing attacks. The detection algorithms, particularly the global multiple AMs, were very successful since it achieved more accurate result than existing approaches. The result showed that the GMM method is robust against antenna diversity and significantly outperformed. **("Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength").**

Shang.L and Arora.A [29] proposed the concept of spatial signature for crypto-free authenticated communication, and a lightweight primitive to realize the concept of security in wireless sensor networks in 2008. Using this primitive, a protocol is designed robustly and validates the authenticity of the source of messages efficiently. Authentic messages incur no communication overhead whereas masqueraded communications are detected cooperatively by the neighboring nodes. The protocol enables lightweight collusion-resistant methods for broadcast authentication, unicast authentication, non-repudiation and integrity of communication. Adding an acknowledgement from the receiver to the cooperative defense protocol is that; it can deal with attacks greatly. The result showed that the accuracy of the proposed primitive is high per packet level. It is also validated the robustness of the primitive. **("Spatial Signatures for Lightweight Security in Wireless Sensor Networks")**

V.Shyamaladevi and Dr.R.S.D. WahidaBanu proposed the Stack Path identification marking technique and filtering mechanism in 2008 [30]. The Stack Path Identification marking scheme consists of two new marking methods Stack-based marking and Write-ahead marking. The proposed scheme almost completely eliminates the effect of legacy routers on a path, and performs better than the original Path identification. Filtering with the Path Identification derives an optimal threshold strategy. The system develops the Path Identification (IP) filter, to detect IP spoofing attacks with just a single attack packet. The result showed that Path Identifier provides measurable DDoS protection in the marking scheme. The Path identification scheme is very general and quite promising in performance. **("Detection of Spoofing Attacks Using Intrusive Filters For DDoS").**

In 2008, Jie Yang and Ying ying Chen proposed RF- based fingerprint matching schemes [31] to quantify the localization accuracy and derive an analytic expression of the Cumulative Distribution Function (CDF) of localization errors. Further the effects of the sampling point's size and the distance between two adjacent sampling points are studied and the mathematical relationship of the localization error to sampling points is derived. The result provides strong evidence for the performance of RF-based fingerprint matching algorithms to quantify the localization. **("A Theoretical Analysis of Wireless Localization Using RF-based Fingerprint Matching").**

Zhenhai Duan et al., proposed an Inter Domain Packet Filter (IDPF) architecture as an effective countermeasure to the IP spoofing based DDoS attacks in 2008 [32]. By using Border Gateway Protocol (BGP), IDPF update the messages exchanged between the neighbor and source address. The IDPFs can easily be deployed on the current BGP-based Internet routing architecture and the IDPF framework can correctly work without discarding any valid packets. Simulation results showed that, IDPFs can significantly limit the spoofing capability of attackers and also help pinpoint the true origin of an attack. **("Controlling IP Spoofing through Interdomain Packet Filters").**

In 2009, Kavitha Muthukrishnan et al., [33] proposed an algorithm called a range of motion detection algorithm. The presented algorithm is evaluated based on classification metrics such as recall and precision obtained and annotated traces over twelve hours. The common deterministic localization algorithms such as centroid and weighted centroid can improve the performance when a motion model is integrated. Motion models are normally used as probabilistic algorithms. The result showed that the motion detection algorithms exploiting the frequency domain characteristics and reported precision and recall over 90%. **("Inferring Motion and Location Using WLAN RSSI").**

In 2009, Jeong Heon Lee and R. Michael Buehrer [34] proposed a localization technique using Differential Received Signal Strength (DRSS). The method does not use signal source cooperation for location estimation. In geometric interpretation, both local and global positioning are used to facilitate the understanding of the approach DRSS. Then, a Least-Squares (LS) optimization framework is formulated for DRSS-based location estimation (DRLE). The result showed that the DRLE has practicaly several advantages over other positioning techniques and the location accuracy of DRLE improves, where most existing positioning techniques may struggle. **("Location Estimation Using Differential RSS with Spatially Correlated Shadowing").**

In 2009, J.Yang et al., [35] proposed a technique DEtecting MObile Spoofing aTtacks in wireless Environments (DEMOTE). Identity-based spoofing attacks are a kind of network threats that facilitate to create a variety of advanced attacks. The method Received Signal Strength (RSS) exploits traces over time and finds an optimal threshold to partition the RSS traces into classes. ALignment Prediction (ALP) algorithm exploits the temporal constraint in the RSS readings and predicts the best RSS alignment of partitioned RSS classes for RSS trace reconstruction. The result showed that DEMOTE achieves accurate attack detection in both signal space and physical space using localization. **("Detecting Spoofing Attacks in Mobile Wireless Environments")**

In 2009, Guenther Lackner et al., [36] proposed finger print technique for detecting the MAC address spoofing in wireless network. The method relies on supervised machine learning algorithms to learn the typical histograms for each chipset. The client uses the chipset which is the target for the analysis and creates traffic by communicating with another machine. The probe captures the traffic in the monitor mode of its WLAN card. The traffic from the client to the server has been generated by using ICMP pings for covering a large range of possible packet sizes. The captured data is used to create histograms for the construction of the training set and the test set. The result showed that the size of the packet does not increase the time delay. **("Combating Wireless LAN MAC-layer Address Spoofing with Fingerprinting Methods").**

Gayathri Chandrasekaran et al., proposed an architectural detection algorithm to detect the identity spoofing attacks robustly in 2009 [37]. Identity spoofing allows an attacker to avail network services that are normally restricted to legitimate users. Several techniques that rely on physical properties of transmitting devices are ineffective for the mobile attacker. The algorithm RSSI-based per-packet localizer employs powerful detectors to identify and eliminate the spoofing attack. The experimental results showed that it effectively detect identity spoofs with a low false positive rate of 0.5%. **("Detecting Identity Spoofs in IEEE 802.11e Wireless Networks").**

In 2010, Jeong Heon Lee and R. Michael Buehrer [38] proposed the statistical and pattern matching techniques and geometric techniques for location spoofing attack detection. The statistical and pattern matching techniques called Relative Error Detection (RED) and Topological Residual Fingerprint Matching (TRFM) are used for detecting both signal strength and beam forming attacks. The geometric filtering is developed to considerably improve reliability of the location by exploiting the geometry of nodes. The result showed that the proposed techniques effectively detect the location of the spoofing attack. **("Location Spoofing Attack Detection in Wireless Networks").**

Liang Xiao et al., proposed a PHY-authentication protocol to detect spoofing attacks in wireless networks in 2010 [39]. Channel estimations systems reduce the workload of the higher-layer process and provide some degree of spoofing protection. Analysis of the results showed that the method can significantly reduce the workload of the higher-layer security mechanism. **("PHY-Authentication Protocol for Spoofing Detection in Wireless Networks").**

F.A. Barbhuiya et al., presented an active Discrete Event Systems (DES) based Intrusion Detection System (IDS) for detecting ARP spoofing in 2011 [40]. The scheme is based on formal state-transition modeling. It is used to analyze all the spoofing attack scenarios which can be and cannot be detected. The scheme also uses an active probing mechanism. It is a software based approach which runs in one host (IDS), does not require any additional hardware or software patching in the hosts. The result showed that the overhead of extra traffic is negligible in DES based IDS. **("An Active DES based IDS for ARP Spoofing").**

In 2011, Ferdous A Barbhuiya et al., [41] proposed an active Host based IDS (HIDS) for ARP to detect large set of ARP related attacks. The scheme uses an active probing mechanism and does not violate the principles of network layering architecture. The scheme can only detect the attacks. In other words, in case of spoofing it can only determine the conflicting IP-MAC pairs without differentiating the spoofed IP-MAC and genuine IP-MAC pair. Also presented network based IDS detect, such spoofing attacks and highlights number of the attackers that are eliminated. The scheme is successfully validated in a test bed with various attack scenarios and the result showed that it effectively detects the ARP related attacks. **("An Active Host-based Intrusion detection system for ARP-related attacks and its verification").**

In 2012, Wesam S. Bhaya and Samraa A. AlAsady [42] introduced a security algorithm which has two parts: Additional Authentication Process and the periodic re-authentication process. When the AP receives an Authentication frame from a client, it first checks the MAC address for its legality; the AP will re-compute the Hash value depending on the corresponding identifiers stored in the access control list and the time of the frame is created. Then compare the resulted hash value with the received one and decide whether to reject or accept. If the attacker is spoofed, the MAC address cannot communicate with the network. The result showed that the periodic re-authentication process makes additional support to the authentication, so the MAC address spoofer will be detected and prevented. **("Prevention of Spoofing Attacks in the Infrastructure Wireless Networks")**

In 2012, Ali Broumandan et al., [43] proposed a spoofing detection method based on a single moving antenna. The spoofing signals generated from a single point source can effectively be detected based on the spatial correlation of the signal parameters. Through a process of sorting the authentic and spoofing signals based on the pair wise signal parameters correlation, it is possible to sort the signals such that only the authentic signals are passed to the navigation solution. A key observation is that the detection performance of the developed method is not affected by spatial multipath fading that the GNSS signals are subjected to. Also the trajectory of the receiver antenna can be random and does not have to be jointly estimated as part of the overall spoofing detection. The result showed that test scenario satisfies the requirements for a real world spoofing experiment without the need for outdoor transmission in the GPS bands. **("GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation").**

In 2013, Jie Yang et al., [44] introduced an spatial correlation of Received Signal Strength (RSS) to sense the spoofing attacks for determining the number of attackers. The Cluster-based mechanisms are used to determine the number of attackers. Training data sets are explored using the Support Vector Machines (SVM) to improve the accuracy. System is constructed by integrative detection and localization to localize the positions of multiple attackers. An advantage of employing spatial correlation is to detect spoofing attacks without any additional cost or modification of the wireless devices themselves. The experimental results showed that the proposed method achieved above 90 percent of Hit Rate and Precision when determining the number of attackers. **("Detection and Localization of Multiple Spoofing Attackers in Wireless Networks")**

Qi Zeng et al., proposed a CUmulative SUM (CUSUM) test algorithm to detect the GPS spoofing attack efficiently in 2013 [45]. The GPS spoofing attack is a type of malicious threat. The CUSUM detection scheme is used for determining the occurrence of GPS spoofing attack as quickly as possible. The simulation result showed that the proposed scheme is an effective method to detect the GPS spoofing attack. **(" GPS Spoofing Attack on Time Synchronization in Wireless Networks and Detection Scheme Design").**

In 2013, Zhenghao Zhang et al., [46] proposed a quickest spoofing detection algorithm for detecting the GPS spoofing attacks. A malicious attacker may spoof a GPS receiver, causing it to provide incorrect navigation and timing information, which may lead to serious damage. GPS is being increasingly used in critical infrastructures in modern society. A monopole patch hybrid antenna is applied to feed received GPS signal into two independent GPS receivers. The standard deviation of the C/No (the Carrier-Signal-to-Noise Ratio) ratio has been exploited to conduct a statistic measurement. The quickest detection algorithm has been applied to detect the time when the spoofing attack occurs based on the output of the C/No statistic measurement. The experimental result demonstrated that the proposed algorithm can effectively detect the spoofing attack when it occurs. **(“Quickest Detection of GPS Spoofing Attack”).**

In 2013, Hao Yang et al.,[47] presented two strategies to detect the intermediate spoofing attackers by analyzing the abnormal signal variations in the receiver. Strategy 1 breaks the receiver tracking states; while Strategy 2 breaks the consistency between the carrier phase and the code phase, in a manner of less likely to alert the receiver. The result showed that the strategy 2 is more successful since it is inexpensive, used by most receivers, requires only a small software upgrade and indicate the receiver when spoofing has occurred. **(“HOURS: Achieving DoS Resilience in an Open Service Hierarchy”).**

In 2014, Ahmed M. Abdel Salam et al., [48] proposed a scalable technique called static ARP entries to prevent ARP spoofing attacks. Every host in the local network has been protected from non-spoofed ARP attack. The technique operates in both static and DHCP based addressing schemes. The scalability of the technique protects the large number of users without any overhead on the administrator. The results showed that the client does not require not more than one millisecond to register itself for a protected ARP cache and the server can block any attacker in just a few microseconds under heavy traffic**. (An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries).**

In 2014, M.Loganathan and V.Navaneethakrishnan [49] proposed the K-means cluster algorithm to detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity and eliminate them. Determining the number of adversaries is particularly a challenging problem. The integration of detection and localization system can localize any number of adversaries even through different transmission power levels are used by attackers. The results providing strong evidence for the effectiveness of the approach in detecting wireless spoofing attacks, determines the number of intruders and to localize the adversaries. **(Detecting and Localizing Wireless Spoofing Attacks).**

In 2014, Archana Shelar and M.D.Ingale [50] proposed the Received Signal Strength (RSS) mechanism and IDOL model. It mainly focused on spoofing attack detection in the network, determines the number of attackers and localizing multiple attackers. The multiclass detection problem is formulated to find number of spoofing attackers. Further the IDOL model is used to localize positions of actual attackers. The experimental results showed that the techniques provide high level of security with topmost hit rate and precision, also it gives the best accuracy for localizing multiple adversaries. **(“Modeling Security with Localization of Multiple Spoofing Attackers in Wireless Network”).**

III. ISSUES IN SPOOFING ATTACK DETECTION

From the review of literature, some of identified spoofing attack issues are given under here.

1). Detect the presence of spoofing attacks,

2). Determine the number of attackers,

3). Localize multiple adversaries and eliminate them.

IV. CONCLUSION

Spoofing attack is one of the major issues in wireless sensor network. The identification of spoofers and localization of the same is a challenging task in wireless sensor network. In this paper, various algorithms are proposed. Spoofing attack detection and localization in wireless sensor network have been extensively studied. There is no unique method for identifying and removing the spoofing attack in the wireless sensor network. Each method has its own advantages and disadvantages. The number of issues such as detecting the presence of spoofing attacks, determining the number of attackers, localizing multiple adversaries and eliminating them are not solved effectively. Further, this paper will help the researcher to invent novel method in order to identify the spoofing attack as well as remove or disable the same in wireless sensor network effectively with less cost.

REFERENCES

[1] Heejo Lee and Kihong Park, “On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack,” In Proceedings IEEE INFOCOM 2000, August 2000.

[2] Balachander Krishnamurthy and Jia Wang, “On network-aware clustering of Web clients,” in SIGCOMM '00 Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pages 97-110, Volume 30 Issue 4, October 2000.

[3] P. Bahl and V.N. Padmanabhan, “RADAR: An in- Building RF- Based User Location and Tracking System,” Proc. IEEE INFOCOM, vol. 2, Page(s): 775 – 784, 2000.

[4] Maurizio A. Spirito, “On the Accuracy of Cellular Mobile Station Location Estimation,” IEEE Transactions On Vehicular Technology, Vol. 50, No. 3, May 2001.

[5] 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.

[6] T. Roos, P. Myllymaki, H.Tirri, P. Misikangas, and J. Sievanen, “A probabilistic approach to WLAN user location estimation,” +International Journal of Wireless Information Networks, vol. 9, no. 3, pp. 155–164, July 2002.

[7] Daniel B. Faria and David R. Cheriton, “DoS and Authentication in Wireless Public Access Networks,” In Proceedings of the First ACM Workshop on Wireless Security (WiSe’02), September 2002.

[8] Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions”, Proc. USENIX Security Symp., pp. 15- 28, August 2003.

[9] Mathias Bohge and Wade Trappe, “An Authentication Framework for Hierarchical Ad Hoc Sensor Networks,” IEEE Trans. Ad Hoc Sensor Networks, WiSE’03, September 19, 2003.

[10] Pradeep Kyasanur and Nitin Vaidya, “Detection and Handling of MAC Layer Misbehavior in Wireless Networks,” In Proceedings the International Conference on Dependable Systems and Networks, San Francisco, CA, June 2003.

[11] P. Tao, A. Rudys, A. Ladd, and D. S. Wallach, “Wireless LAN Location-Sensing for Security Applications,” In Proc. of the Second ACM Workshop on Wireless Security (WiSe'03), pages 11-20, Sept. 2003.

[12] Hao Yang, Haiyun Luo, Yi Yang, Songwu Lu and Lixia Zhang, “HOURS: Achieving DoS Resilience in an Open Service Hierarchy,” proc. IEEE Global Telecommunications Conference (GLOBECOM), 2003.

[13] Minho Sung and Jun Xu, “IP Traceback-based Intelligent Packet Filtering: A Novel Technique for Defending Against Internet DDoS Attacks,” IEEE Transactions On Parallel and Distributed Systems, Vol. 14, No. 9, September 2003.

[14] 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.

[15] J.Hall, M.Barbeau, and E.Kranakis, “Enhancing IntrusionDetection in Wireless Networks Using Radio Frequency Fingerprinting,” In Proc. of The IASTED Conference on Communications, Internet and Information Technology, Nov. 2004.

[16] 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.

[17] 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.

[18] Yang Xiao, Chaitanya Bandela and Yi Pan, “Vulnerabilities and Security Enhancements for the IEEE 802.11 WLANs,” proc. IEEE Global Telecommunications Conference (GLOBECOM), 2005.

[19] 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.

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

[21] 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.

[22] Kai Zeng, Kannan Govindan, Daniel Wu, Prasant Mohapatra,” Identity-Based Attack Detection in Mobile Wireless Networks,” IEEE INFOCOM, Page(s): 1880 – 1888, 2011.

[23] Fanglu Guo, Jiawu Chen and Tzi-cker Chiueh, “Spoof Detection for Preventing DoS Attacks against DNS Servers,” 26th IEEE International Conference on Distributed Computing Systems (ICDCS), 2006.

[24] Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wireless spoofing attacks,” in SECON’07: Proceedings of the 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 2007.

[25] Xiao L and Trappe W, “Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,” Proceedings of IEEE International Conference on Communications (ICC), pp. 4646-4651, 2007.

[26] Qing Li and Wade Trappe, “Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationship,” IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, December 2007.

[27] Ruiliang Chen, Jung-Min Park and Randolph Marchany, “A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks,” IEEE Transactions on Parallel And Distributed Systems, Vol. 18, No. 5, May 2007.

[28] Y. Sheng, K. Tan, G. Chen, D. Kotz and A. Campbell, “Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength,” Proc. IEEE 27th IEEE International Conference on Computer Communications (INFOCOM), Apr. 2008.

[29] Lifeng Sang and Anish Arora, ”Spatial Signatures for Lightweight Security in Wireless Sensor Networks,” proc. IEEE INFOCOM, page 2137-2145, 2008.

[30] V.Shyamaladevi and Dr.R.S.D. WahidaBanu, ”Detection of Spoofing Attacks Using Intrusive Filters For DDoS,” IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008.

[31] Jie Yang and Yingying, “A Theoretical Analysis of Wireless Localization Using RF-based Fingerprint Matching,” IEEE International Symposium on Parallel and Distributed Processing, (IPDPS), page 1-6, 2008.

[32] Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar, “Controlling IP Spoofing through Interdomain Packet Filters,” IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 1, January-March 2008.

[33] Kavitha Muthukrishnan, Berend Jan van der Zwaag, and Paul Havinga, “Inferring Motion and Location Using WLAN RSSI,” proc. IEEE INFOCOM, 2009.

[34] J. H. Lee and R. M. Buehrer, “Location estimation using differential RSS with spatially correlated shadowing,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), November, 2009.

[35] J. Yang, Y. Chen, and W. Trappe, “Detecting Spoofing Attacks in Mobile Wireless Environments,” Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2009.

[36] G Äuenther Lackner, Udo Payer and Peter Teu, “Combating Wireless LAN MAC-layer Address Spooing with Fingerprinting Methods,” proc IEEE International Journal of Network Security, Vol.9, No.2, PP.164-172, Sept. 2009

[37] Gayathri Chandrasekaran, John-Austen Francisco, Vinod Ganapathy, Marco Gruteser and Wade Trappe, “Detecting Identity Spoofs in IEEE 802.11e Wireless Networks,” proc. IEEE GLOBECOM, 2009.

[38] Jeong Heon Lee and R. Michael Buehrer, ”Location Spoofing Attack Detection in Wireless Networks,” proc. IEEE GLOBECOM, 2010.

[39] Liang Xiao, Alex Reznik, Wade Trappe, Chunxuan Ye, Yogendra Shah, Larry Greenstein and Narayan Mandayam, “PHY-Authentication Protocol for Spoofing Detection in Wireless Networks,” proc. IEEE Global Telecommunications Conference (GLOBECOM), 2010.

[40] F.A. Barbhuiya, S Biswas and S Nandi, “An Active DES based IDS for ARP Spoofing,” IEEE International Conference on Systems, Man, and Cybernetics (ICSMC), Page(s): 2743 – 2748, 9 Oct 2011.

[41] Ferdous A Barbhuiya, Santosh Biswas and Sukumar Nandi, “An Active Host-based Intrusion detection system for ARP-related attacks and its verification”, IEEE Trans. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[42] Wesam S. Bhaya and Samraa A. AlAsady, ”Prevention of Spoofing Attacks in the Infrastructure Wireless Networks,” proc IEEE Journal of Computer Science 8 (10): Page(s): 1769-1779, 2012.

[43] Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen and Gérard Lachapelle, “GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation,” IEEE/ION PLANS April 24-26, 2012.

[44] Jie Yang, Yingying Chen and Wade Trappe, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks”, IEEE Transaction on parallel and distributed system, Vol. 24, NO. 1, January 2013.

[45] Qi Zeng, Husheng Li and Lijun Qian, “GPS Spoofing Attack on Time Synchronization in Wireless Networks and Detection Scheme Design,” proc. IEEE MILCOM, Page(s): 1 – 5, 2012.

[46] Zhenghao Zhang, Matthew Trinkle, Lijun Qian and Husheng Li, “Quickest Detection of GPS Spoofing Attack,” Proc. IEEE Military Communications Conference (MILCOM), Page(s): 1 – 6, 2012.

[47] Hao Yang, Haiyun Luo, Yi Yang, Songwu Lu and Lixia Zhang, “HOURS: Achieving DoS Resilience in an Open Service Hierarchy,” proc. IEEE Global Telecommunications Conference (GLOBECOM), 2003.

[48] Ahmed M.AbdelSalam ,Wail S.Elkilani and Khalid M.Amin, “An Automated approach for Preventing ARP Spoofing Attack using Static ARP Entries” Proc IEEE (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.

[49] M .Loganathan and V.Navaneethakrishnan, ”Detecting and Localizing Wireless Spoofing Attacks” IEEE Trans. International Journal of Advanced Research in Computer Science and Software Engineering vol4 Iss2, pp. 374-381, February 2014.

[50] Archana Shelar and M.D.Ingale, ”Modeling Security with Localization of Multiple Spoofing Attackers in Wireless Network,” The International Journal Of Engineering And Science (IJES), Volume 3, Issue 01, Pages 01-06, 2014.

[51] Jie Yang, Yingying Chen, and Jerry Cheng, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks” in IEEE 2012.

[52] Mukesh Barapatre, Prof. Vikrant Chole and Prof. L. Patil, “A Review on Spoofing Attack Detection in Wireless Adhoc Network”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 6, November – December 2013.