iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** II **Month of publication:** February 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Evolution and Performance Analysis of Multiple Spoofing Attackers in Wireless Networks

P. Kiruthika Devi[1], Dr. R. Manavalan[2]
[1]Research Scholar in Department of Computer Science, [2]Head of the Department of Computer Applications,
K.S.Rangasamy College of Arts and Science, Tiruchengode-637215, India

Abstract--Spoofing attack is an identity based attack through which a malicious user can spoof the MAC address of an node to create multiple illegitimate identities that highly affect the performance of wireless sensor network. The identification of spoofing attackers, determining the number of attackers, localizing multiple adversaries and eliminating them is a challenging task in Wireless Sensor Network. The K-Means clustering approach is used to detect the spoofing attackers and localize them. This approach did not predict the attackers accurately. To overcome this problem, this paper proposes Chronological Likelihood Fraction Test (CLFT) as a fast and effective mobile replica node detection scheme to detect the spoofing attackers when the node is fixed or in movement. In addition, it uses the inherited spatial correlation of Received Signal Strength (RSS) from wireless nodes to detect the spoofing attacks. It formulates the problem of determining the number of attackers as a multi class detection problem. The Support Vector Machines (SVM) method is used to train the data to further improve the accuracy of determining the number of attackers. Analytical and simulation experiments result shows that the proposed scheme detects the attackers in Wireless Sensor Network in an efficient and robust manner at the cost of reasonable overheads.
Keywords-- Wireless network security, spoofing attack, attack detection, localization

I. INTRODUCTION

Wireless networks can be deployed in hostile environments where adversaries may be present. Wireless networks are usually deployed in an unattended manner and are controlled remotely by the network operator [22]. The unattended nature of wireless networks can be exploited by attackers. Specifically, an attacker can capture and compromise wireless nodes and launch a variety of attacks by leveraging compromised nodes [23]. Significant fraction of the network traffic is monitored and would pass through the compromised nodes. Alternatively, falsified data is injected to corrupt monitoring operation of the sensors. A more aggressive attacker could not be determined by common sensor network protocols, including cluster formation, routing, and data aggregation, thereby causing continual disruption to the network operations [24]. Therefore, an adversary with compromised nodes can paralyze the deployed mission of wireless networks. In this sense, it is very important to detect and revoke compromised nodes as early as possible in the network. Spoofing attacks can further facilitate a variety of traffic injection attacks [1], [2], such as attacks on access control lists, rogue access point attacks, and eventually Denial-of- Service (DoS) attacks. A broad survey of possible spoofing attacks can be found in [3], [4]. Moreover, in a large-scale network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks such as network resource utilization attack and Denial-of-Service attack quickly. Therefore, it is important to i). Detect the presence of spoofing attacks, ii). Determine the number of attackers, and iii). Localize multiple adversaries and eliminate them.
Most of the approaches have been introduced so for to address potential spoofing attacks based on cryptographic schemes [5], [6]. However, cryptographic schemes based applications require reliable key distribution, management, and maintenance mechanisms. It is not always desirable since it's infrastructural, computational and management overhead. The use of RSS-based spatial correlation and a physical property associated with each wireless node is hard to falsify and not relevant on cryptography for detecting spoofing attacks. Attackers who have different locations than legitimate wireless nodes are concerned, spatial information is used to not only identify the presence of spoofing attacks but also localize adversaries [25]. Spatial correlation is highly employed to detect spoofing attacks in wireless sensor network without any additional cost or modification to the wireless devices themselves. The overview of the proposed model is discussed in section 1.1.

A. Overview of proposed model

Fig. 1, shows overview of the proposed model. The Base station collects the information from the wireless nodes. The spatial correlation of Received Signal Strength (RSS) is used to detect the spoofing attacks. The K-Means clustering approach and Chronological Likelihood Fraction Test (CLFT) are implemented to determine the number of spoofing attack and localize them in wireless sensor network. Further SVM is used to improve the accuracy of determining the number of attackers.

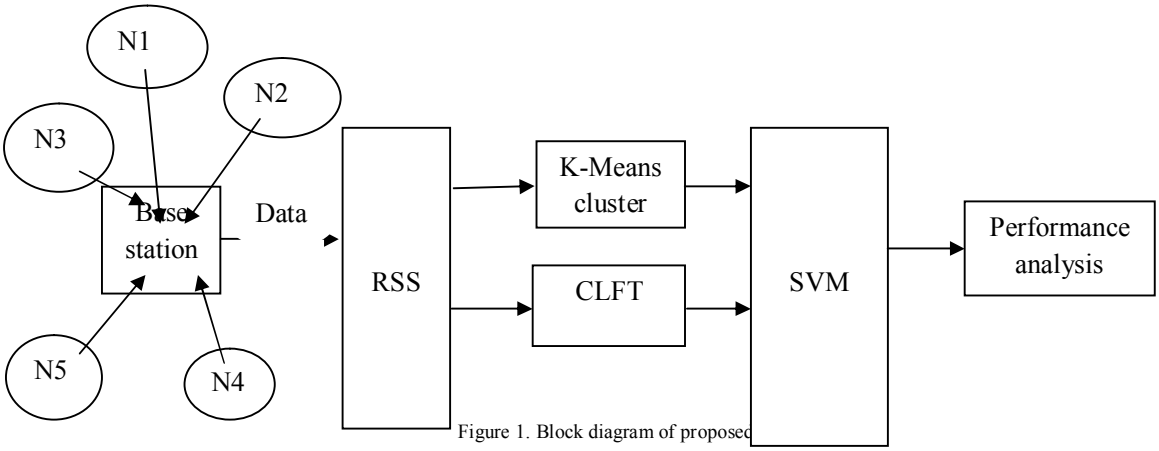


Figure 1. Block diagram of proposed

The rest of this paper is arranged as follows: In Section II some related works are discussed. The problem statement is described in Section III and Section IV, discusses about the Medium Access Control protocol, the enhanced framework for detecting and localizing the spoofing attack is presented in section V. In Section VI, the performance analysis of the proposed framework is discussed. Section VII provides the final conclusion with future scope.

II. RELATED METHOD

To prevent spoofing attacks, cryptographic based authentication [5], [10], [11] is used traditionally. Wu et al. [5] have introduced a Secure and Efficient Key Management (SEKM) framework. In SEKM, Public Key Infrastructure (PKI) is built by applying a secret sharing scheme and an underlying multicast server group. Wool [10] implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys.
A channel-based authentication scheme was proposed by M. Bohge and W. Trappe to discriminate between transmitters at different locations and detect spoofing attacks in wireless networks [12]. Brik et al. [13] focused on building fingerprints of 802.11bWLAN NICs by extracting radiometric signatures, such as frequency magnitude, phase errors, and I/Q origin offset, to defend against identity attacks. Li and Trappe [14] introduced a security layer that used forge-resistant relationships based on the packet traffic, including MAC sequence number and traffic pattern, to detect spoofing attacks.

Received Signal Strength is used to defend against spoofing attacks [15], [16], [17]. Faria and Cheriton [15] proposed Wired Equivalent Privacy (WEP) encryption technique which provides key management to address host-revocation problem. Sheng et al. [16] proposed the RSS readings using a Gaussian mixture model. Sang and Arora [17] proposed “spatial signature” in which the node including Received Signal Strength Indicator (RSSI) and Link Quality Indicator (LQI) are used to authenticate messages in wireless networks.
P. Bahl and V.N. Padmanabhan [18] proposed and demonstrated the method RADAR for identifying the location of attacker in wireless sensor network. Shang.L and Arora.A [19] 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.
C. Hsu and C. Lin [20] proposed the concept of ‘Support Vector Machine’ which is originally designed for binary classification and it is also used to solve multiclass problems. Daniel B. Faria and David R. Cheriton [21] proposed the mobility-aware access control mechanism which is more suitable for both wireless and wired environments.
However, none of these approaches are suitable for determining the number of attackers when multiple adversaries collectively use the same identity to launch malicious attacks. There is no ability to localize the positions of the adversaries after attack is detected. None of the existing work can determine the number of attackers when there are multiple adversaries spoof the same identity. Additionally, the proposed approach can accurately localize multiple adversaries even through the attackers are varying in their transmission power levels to spoof the system of their true locations.

III. PROBLEM DESCRIPTION

Inaccurate estimation of the number of attackers will cause failure in localizing the multiple adversaries. It is hard to know how many adversaries will use the same node identity to launch attacks, determining the number of attackers becomes a multiclass detection problem and it is similar to determining how many clusters exists in the RSS readings. If C is the set of all classes, i.e.,

all possible combination of the number of attackers, C= {1, 2, 3, 4}. For a class of specific number of attackers c_i, e.g., c_i =3, P_i is defined as the positive class of c_i and all other classes as negative class N_i

$$P_i = c_i$$
$$N_i = \bigcup_{j \neq i} c_i \in C$$

The number of attackers can be accurately determined over all possible testing attempts with mixed number of attackers. Associated with a specific number of attackers i, the Hit Rate is defined as $HR_i = \frac{N_{true}}{P_i}$ where N_{true} is the true positive detection of class c_i. Let N_{false} be the false detection of the class c_i out of the negative class N_i that do not have i number of attackers. The false positive rate FP_i for a specific number of attackers of class c_i is defined as $FP_i = \frac{N_{false}}{N_i}$. Then, further the multiclass ROC graph is used to measure the effectiveness of our mechanisms. Particularly, we use two methods are used: class- references based and benefit error based. The class-reference-based method produces C different ROC curves when handling C classes by using Pi and Ni. Further, in the C- class detection problem, the traditional 2 x2 confusion matrix, including True Positives, False Positives, False Negatives, and True Negatives, becomes an C x C matrix, which contains the C benefits (true positives) and C2 - C possible errors (false positives). The benefit-error-based method is based on the C x C matrix. For example, when C = 3 with possible number of attackers of {2, 3, 4}, the benefits are 3 and the possible errors are 6.

IV. MEDIIM ACCESS CONTROL (MAC) PROTOCOL

When multiple nodes try to send messages simultaneously over the same medium, only one node can be send successfully. MAC protocols are used for solving this contention problem. MAC protocols are mainly divided into two categories: distributed MAC protocols and centralized MAC protocols based on a control center is required for the protocol. Protocols can be further classified based on the mode of operation into Random Access Protocols, Guaranteed Access Protocols, and Hybrid Access protocols. In a random access protocol, nodes are accessed to the medium. When only one node makes a transmission attempt, the packet is delivered successfully. When multiple nodes attempt the same transmission, a collision occurs. Nodes resolve the collisions in according to rules defined by the Contention Resolution Algorithm (CRA).

In a guaranteed access protocol, nodes access the medium in a round-robin fashion. These protocols are implemented in one of 2 ways. One is master-slave configuration called as polling protocols where as the second one token-passing protocol operates in a distributed manner by exchanging tokens.

Hybrid Access Protocols blend the best qualities of the above two protocols to derive more efficient MAC protocols. Most hybrid Access Protocols are based on request-grant mechanisms which sent the request using a random access protocol. The base station then allocates an upstream time slot for the actual data transmission and sends a grant to the node in that time slot.

V. RECEIVED SIGNAL STRENGTH (RSS)

For spoofing detection, strategies are devised which use the uniqueness of spatial information, instead of using the location directly because the attacker's positions are unknown. RSS is a property closely correlated with location in physical space and is readily available in the wireless network. Even though it was affected by random noise, multipath effects, and environmental bias, received signal strength is measured at a set of landmarks reference points with known locations, closely associated with the transmitter's physical location and is governed by the distance to the landmarks. The RSS readings at different physical location are distinctive, whereas the RSS readings at same locations in physical space are similar. Thus, the RSS readings present strong spatial correlation characteristics. The RSS value vector as S = $(S_1, S_2, \ldots, S_n)$ where n is the number of landmarks/access points that monitors the RSS of the wireless nodes and know their locations. Generally, the RSS at the i^{th} landmark from a wireless node is distributed as

$$s_i(d_j)[dBm] = P(d_0)[dBm] - 10\gamma \log\left(\frac{d_j}{d_0}\right) + X_i$$

where $P(d_0)$ represents the transmitting power of the node at the reference distance d_0, d_j is the distance between the wireless node j and the i^{th} landmark, and $\log\left(\frac{d_j}{d_0}\right)$ is the path loss exponent, X_i is the shadow fading which is given as an input. Assume that the wireless nodes have the same transmission power. The following section discusse the existing K-Means clustering approach and the proposed Chronological Likelihood Fraction Test approach.

A. Attack Detection Using K-Means Cluester Anaysis.

The RSS-based spatial correlation is inherited from wireless nodes for spoofing attack detection. The RSS readings from a wireless node may be fluctuated and clustered together. 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 form different clusters in signal space.

Under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings are measured for each individual node (i.e., spoofing node or victim node). Thus spoofing detection is formulated as a statistical significance testing problem, where the null hypothesis is H0: normal (no spoofing attack). In significance testing, a test statistic **T** is used to evaluate whether observed data belong to the null-hypothesis or not. The K-Means clustering algorithm for attack detection in wireless sensor network is given in the figure 2.

K-Means clustering for attack detection in Wireless Sensor Network
INPUT : Assign the closest centroid for each cluster and Get the location information from all the nodes **OUTPUT:** Cluster the nodes
Step 1: Assign each nodes to the group that has the closest centroid. Step 2: Calculate the distance from the data point to each cluster. Step 3: If the data point is closest to its own cluster, leave it where it is. If the data point is not closest to its own cluster, move it into the closest cluster. Step 4: Repeat the Steps 2 and 3 until a complete pass through all the data points results in no data point moving from one cluster to another. Step 5: At this point the clusters are stable. Step 6: At the end collection of nodes are partitioned into K clusters and the data points are randomly assigned to the clusters.

Figure 2: K-Means clustering for attack detection in WSN

B. Chronological Likelihood Fraction Test (CLFT) Approach

The Chronological Likelihood Fraction Test (CLFT) is a statistical hypothesis testing mechanism in which the average number of observations is used to take a decision among all sequential and non-sequential test processes. First the network is divided into a set of zones, establish trust levels for each zone, and detect untrustworthy zones by using the Chronological Likelihood Fraction Test (CLFT). CLFT can be thought of one dimensional random walk with lower and upper limits.

Before the random walk starts, null and alternate hypotheses are defined in such a way that the null one is associated with the lower limit and the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation. If the walk reaches or exceeds the lower or upper limit, the null or alternate hypothesis is selected. The CLFT construct a random walk with two limits in such a way that each walk is determined by the observed speed of a mobile node, the lower and upper limits are properly configured to be associated with the shortfall and excess of the maximum speed of the mobile node.

Each time a mobile sensor node moves to a new location, each of its neighbors asks for a signed claim which contain its location and time information and decides whether to forward the received claim to the base station. The base station computes the speed from every two successive claims of a mobile node and performs the CLFT by taking speed of an observed sample. Each time, maximum speed of the node is exceeded by the mobile node; it will expedite the random walk to hit or cross the upper limit and thus lead to the base station accepting the alternate hypothesis that the mobile node has been replicated. On the other hand, each time the maximum speed of the mobile node is not reached, it will expedite the random walk to hit or cross the lower limit and thus lead to the base station for accepting the null hypothesis that mobile node has not been replicated.

Once the base station decides the replication of mobile node is replicated, it initiates revocation on the replica nodes. The false positive and false negatives are minimized by hypothesis testing to make decisions quickly and accurately. Once a zone is

determined as untrustworthy, the base station or the network operator performs software attestation against all nodes in the untrustworthy zone, detects compromised nodes with subverted software modules, and physically revokes them.

Chronological Likelihood Fraction Test for attack detection in WSN:
INPUT : Get the location information L and time information *T* of the node.
OUTPUT: Accept the hypothesis *H0* or *H*1 for finding the attackers

DECLARATION: *n*=0, *wn*=0
Step 1: Assign the current location and time information for the mobile node
curr_loc=*L,* curr_time=*T*
if *n*>0 then
compute *T0(n)* and *T1(n)*
Step 2: compute the speed 0 from curr_loc and prev_loc, curr_time and prev_time of the mobile node
if 0>*Vmax* then
wn=*wn*+1, **end if**
if *wn*>=*T1(n)* then
Step 3: Accepts the hypothesis *h1* and terminate the test
end if
if *wn*<=*T0(n)* then
Step 4: Initialize *n* and *wn* to 0 and accepts the hypothesis *H0*
return; **end if**
end if *n*=*n*+1
Step 5: Compare the previous and current location and time information of the mobile node
Pre_loc = curr_loc
Prev_time = curr_time

Figure 3: CLFT for attack detection in WSN

The main benefit of this zone-based detection approach is rapid compromise node detection and revocation while saving the large amount of time and effort. By detecting in entire zone at once, the system can identify the approximate source of bad behavior and react quickly, rather than waiting for a specific node to be identified. When multiple nodes are compromised in one zone, then the attackers can be detected and revoked at one time for all.

C. Support vector machine (svm) based mechanism.

SVM method is kernel based learning method which is introduced for classification. It consists of training phase and testing phase. Each data request in the training set consists of a target value and several attributes. Support vector method is used to improve the accurateness of determining the number of attackers. This method collects the training data during the offline period and also increases number of spoofing attacker's detection. The performance of determining number of spoofing attackers can be improved further by using SVM based mechanism. SVM is used to combine the intermediate results (i.e. features) from different statistic methods to build a model based on training data acquired from cluster, to precisely expect the number of attackers. When detecting an attacker in the wireless network, SVM increment the target Value by 1, else 0. The thresholds of test statistics define the critical region for the significance testing. Appropriately setting a threshold τ enables the attack detector to be robust to false detections. The threshold of test can be obtained by the formula $\tau = 2\delta^2 F^{-1}_{\lambda^2(n,\lambda/2\delta^2)}(1-DR)$, the mutual information is nothing but the collection of common information from all other nodes.

SVM for attack detection in Wireless Sensor Network
INPUT : Cluster A, B and C from the dataset.
OUTPUT: Accurately predict the number of attackers.

Step 1: Select the two clusters A and B and compute the cluster centers.
Step 2: Import a new class C from the dataset.
Step 3: Compute the distance between the two clusters A and B.
Step 4: If (d(A,B)>d(A,C) then
B is assigned as normal
C is assigned as attacker
Step 5: calculates the min and max distance between the clusters.
Step 6: If (d(A,B)<threshold limit of the distance) then it creates s new cluster and this is the center of the new cluster
Else B is assigned as a suspected cluster
Step 7: Now compute the mutual information value of all nodes and check it with a threshold.
Step 8: If it is the mutual information value $\geq$ threshold then
Accept the information.
Else Reject the information.

Figure 4: SVM for attack detection in WSN

VI. EXPERIMENTAL ANALYSIS

Simulations are conducted to analyze the performance of proposed model Chronological Likelihood Fraction Test (CLFT) for spoofing attack detection. The described K-Means cluster and CLFT algorithm in previous sections are implemented using C# .Net language and analyzed in the context of spoofing attack detection and localization. The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet. The execution approved out using a cluster environment of 25 wireless mobile nodes over a simulation area of 1200 meters x 1200 meters level gap in service for 60 seconds of simulation time. Each node sends the packet information to the base station in the size of 512 bytes.

Table 1.Simulation Parameters

Parameters	Value
Version	C# .NET
Number of Zone ID	ID1, ID2,ID3,ID4
Simulation Area	1200m x 1200m
Broadcast Area	250 m
Data size	512 bytes
Simulation time	580 sec
MAC Protocol	IEEE 802.11

The parameters such as Error Rate, Precision, F-measure, Hit Rate are used to evaluate the performance of the proposed method for detecting and localizing spoofing attack in wireless sensor network. The parameters and their formulae are shown in Table 2.

Table 2: Parameters with their Formulae

Parameters	Formulae
Error Rate	$ER = s_i(d_j)[dBm] = P(d_0)[dBm] - 10\gamma \log\left(\frac{d_j}{d_0}\right) + X_i$
Precision	$\text{Precision}_i = \frac{N_{true}}{N_{true} + N_{false}}$
F-measure	$F - measure_i = \frac{2}{\frac{1}{\text{Precision}_i} + \frac{1}{HitRate_i}}$
Hit Rate	$HR_i = \frac{N_{true}}{P_i}$

where N_{true} is the true positive detection of class c_i, N_{false} be the false detection of the class c_i, P_i as the positive class. At the time of attack detection, localization error is occurred. The error rate can be calculated using the RSS mechanism. The RSS vector value S = $(S_1, S_2, \ldots, s_n)$ where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations.

Table 3: Error Rate Table

Error Rate	K-Means clustering	Chronological Likelihood Fraction Test
1	8.66	6.7
2	10.33	8.1
3	12.9	10.11
4	18	16.5
5	20.25	18
6	25.33	24
7	30.11	29

The error rate achieved by Chronological Likelihood Fraction Test (CLFT) and K-Means clustering approach is given in table 3. From the simulation results, it is noted that the CLFT technique decreases the error rate when compared with the K-Means Clustering approach for different set of zone ID's. From the table it is proved the CLFT effectively detects the attackers and eliminate them and also decreases the error rate. The Chronological Likelihood Fraction Test (CLFT) approach minimizes the error more than 2% than the K-Means Clustering algorithm. For example, the error rate of the K-Means clustering is 8.66% in the Zone ID 1 where as the CLFT technique decreases the error rate from 8.66 to 6.7% for the same Zone ID at the time of attack detection and localization. The CLFT approach reduces the error 2% - 5% than the K-Means clustering approach and the diagrammatic representation of the same also given in Fig5.

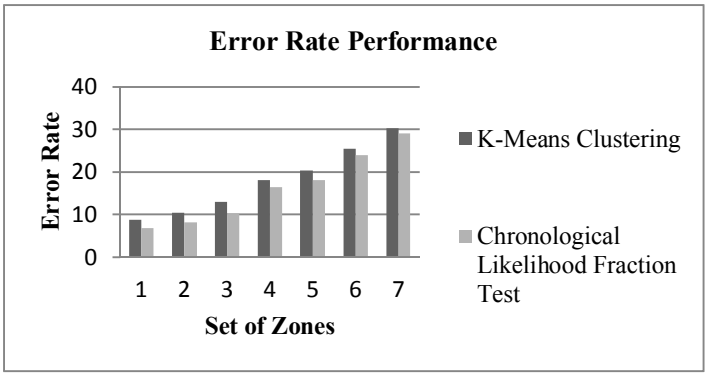


Figure 5: Error Rate performance.

Hit Rate, Precision and F-Measure values

The precision and F-measure values are used in SVM for determining the number of attackers. The advantage of using SVM is that it can combine the intermediate results (i.e., features) from different statistic methods to build a model based on training data to accurately predict the number of attackers. The Precision value is used in SVM for determining the number of attackers. Precision or positive predictive value is defined as the proportion of the true positives results against all the positive results.

Table 4: Precision values of different attackers

Attackers	K-Means Clustering	Chronological Likelihood Fraction Test
2	90.50%	91.54%
3	93.61%	94.64%

4	96.80%	97.82%

From the simulation results, it is noted that the high precision value is achieved by the CLFT technique. The Chronological Likelihood Fraction Test yields higher precision rate compared to K-Means Clustering approach. The CLFT approach detects the number of attackers effectively when compared with other approaches. The results in the table 4 show the precision values earned by the CLFT and the K–means clustering approach and the same is flashed in Fig 6.

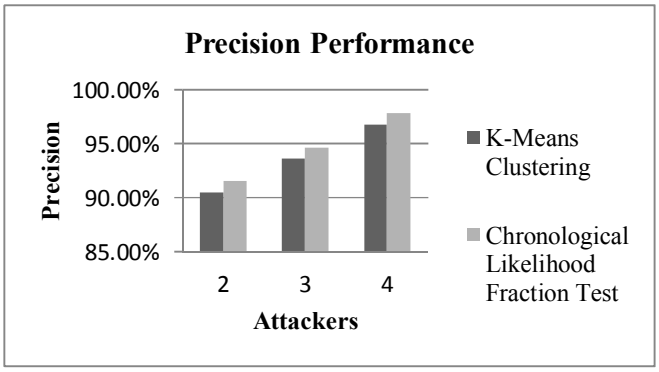


Figure 6: Precision performance of different attackers.

For example if the number of attacker is 2, the number of attack detection precision value is 90.50% in the K-Means Clustering approach where as the number of attack detection precision value of CLFT approach is91.54% which is increased to 1.02%. The proposed CLFT approach achieves more than 1.04% better result than the K-Means Clustering approach.

F-measure: F-measure is computed from information retrieval and measures the accuracy of a test by considering both the Hit Rate and the Precision. The F-measure is used to represent the accuracy of the cluster.

Table 5: F-measure values of different attackers

Attackers	K-Means Clustering	Chronological Likelihood Fraction Test
2	91.54%	92.56%
3	94.34%	95.36%
4	95.30%	95.34%

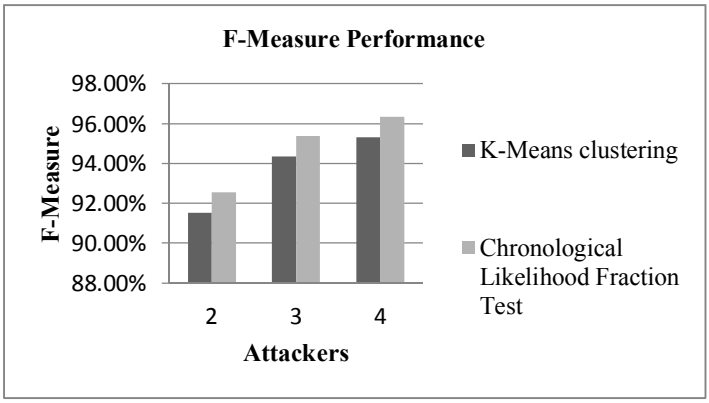


Figure 7: F-measure performance of different attackers.

From the simulation results, it is observed that CLFT achieves high F-measure value when compared with the K-Means Clustering approach. The results in the table 5 show the F-measure value for both CLFT and the K–means clustering approach and the same is projected in the fig 7. For the number of attacker 2, the K-Means Clustering approach yields the F-measure 91.54% where as the CLFT approach achieves 92.56%. The proposed CLFT approach achieves 1.02% higher than the K-Means Clustering approach.

Hit Rate: The Hit rate is nothing but the successive rate of determining the number of attackers. The training data collected during the training phase further improve; the performances of determining the number of spoofing attackers. The Chronological Likelihood Fraction Test (CLFT) detects the number of attackers and achieves the good successive rate when

compared to the K-Means clustering approach.

Table 6: Hit Rate values of different attackers

Attackers	K-Means Clustering	Chronological Likelihood Fraction Test
2	94.82%	95.05%
3	96.95%	97.11%
4	98.12%	98.85%

From the simulation results, it is noted that high successive rate is achieved by the CLFT technique. The Chronological Likelihood Fraction Test earns higher hit rate when compared with the K-Means Clustering approach. The CLFT approach detects the number of attackers and their locations effectively when compared with other approaches. The hit rate of CLFT and the K–means clustering approach is presented in table 6 and the same is flashed in fig 8. For example if the number of attacker is 2, the attack detection hit rate of the K-Means Clustering approach is 94.82% where as the attack detection hit rate of CLFT approach achieves 95.05%. The proposed CLFT approach is 0.23% higher than the K-Means Clustering approach.

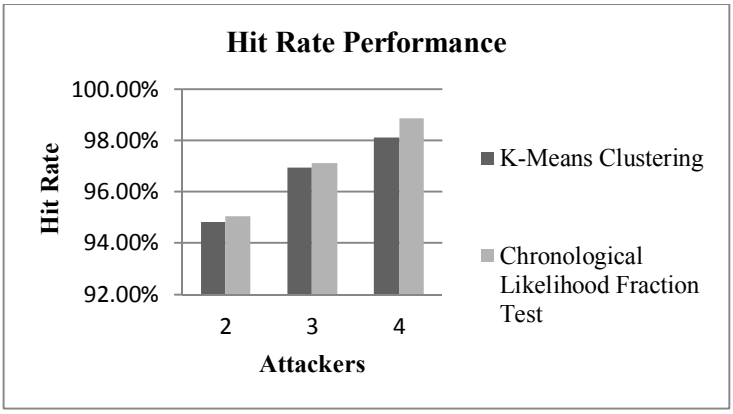


Figure 8: Hit Rate performance of different attackers.

VII. CONCLUSION

In this paper the Chronological Likelihood Fraction Test (CLFT) scheme is proposed for detecting and localizing the spoofing attack in Wireless Sensor network. The performance of spoofing attack detection and localization approaches such as K-Means clustering algorithm and Chronological Likelihood Fraction Test Algorithms are analyzed in 802.11 networks in WSN. Results revealed that the proposed Chronological Likelihood Fraction Test Approach is better for detecting and localizing the misbehaved nodes and eliminate the same. It is a zone based node detection scheme. The proposed mechanism achieves higher accuracy of determining the number of attackers and localizes the attackers than K-Means methods. The experimental result also proved that the proposed scheme quickly detects the untrustworthy zones with zone-trust reports. Further, this scheme may be proposed to evaluate against various types of attacker models and researchers may concentrate on spoofing attack detection and localization to facilitate high result than the other.

REFERENCES

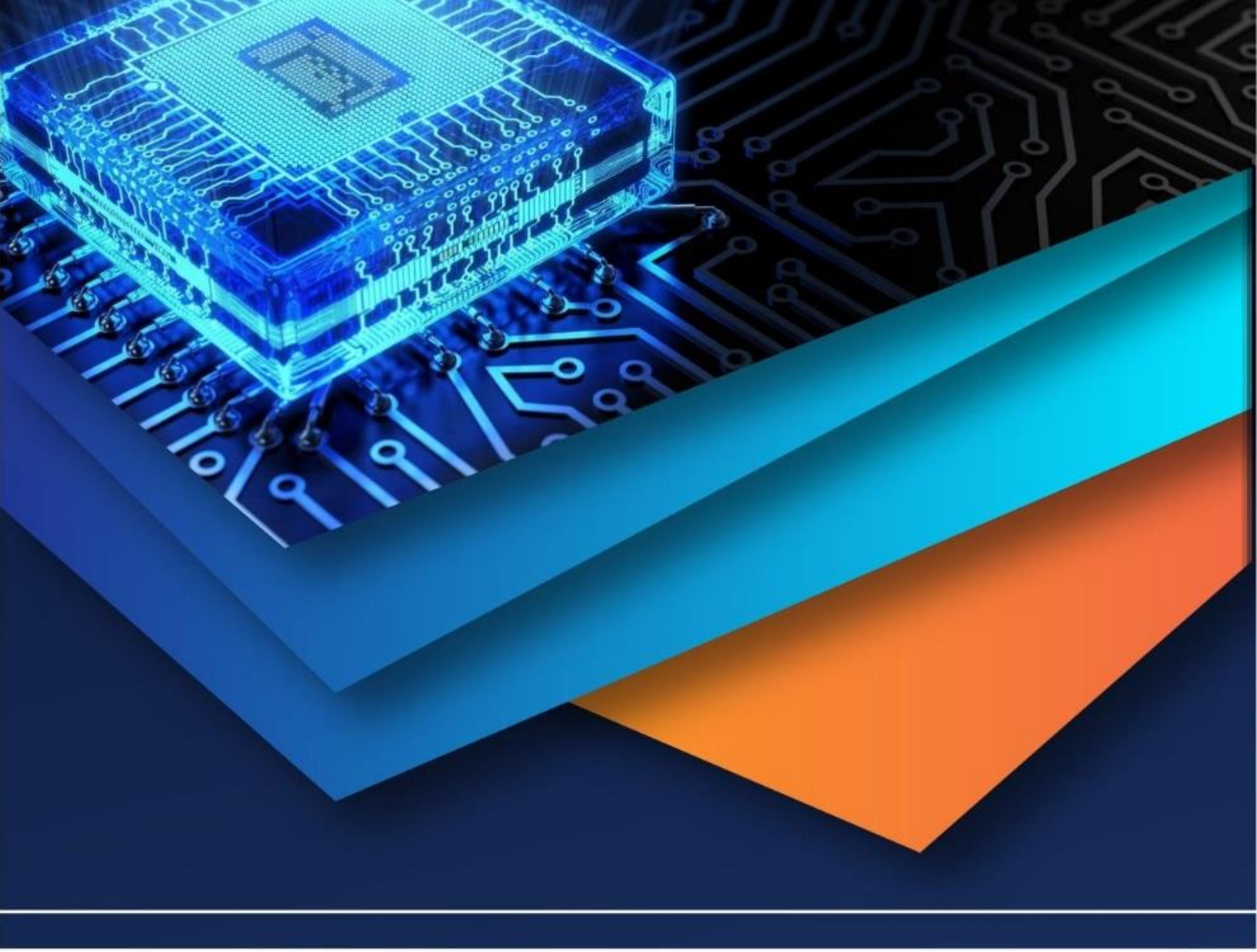
[1]. Jie Yang, Yingying Chen, and Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" in IEEE 2012.
[2]. J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proceedings of the USENIX Security Symposium, 2003, pp. 15 – 28.
[3]. F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access points vulnerabilities to dos attacks in 802.11 networks," in Proceedings of the IEEE Wireless Communications and Networking Conference, 2004.
[4]. D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.
[5]. Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proc. IEEE SECON, 2006.
[6]. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in Proc. IEEE IPDPS, 2005.
[7]. 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.
[8]. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proc. IEEE INFOCOM*, April 2008.
[9]. J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in *Proc. IEEE SECON*, 2009.

[10]. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in *Proc. IEEE IPDPS*, 2005.
[11]. Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wirelss spoofing attacks," in *Proc. IEEE SECON*, May 2007.
[12]. M. Bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003, pp. 79–87.
[13]. V.Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures".
[14]. D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.
[15]. Bahl and V.N.Padmanabhan, "RADAR: An in-Building RF-Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.
[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]. Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc.IEEE INFOCOM, Apr.2007.
[18]. P. Bahl and V.N. Padmanabhan, "RADAR: An in- Building RF- Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000, Page(s): 775 - 784 vol. 2.
[19]. L.Sang and A.Arora, "Spatial Signatures for Lightweight Security in wireless Sensor Networks",Proc. IEEE INFOCOM, pp.2137-2145, 2008.
[20]. 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.
[21]. 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.
[22]. S. Capkun and J.P. Hubaux. Secure positioning in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):221–232, February 2006.
[23]. J. Ho, D. Liu, M. Wright, and S.K. Das, "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.
[24]. Jeong Heon Lee and R. Michael Buehrer, "Location Spoofing Attack Detection in Wireless Networks," proc. IEEE GLOBECOM, 2010.
[25]. 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.

AUTHOR'C BIOGRAPHY

P.Kiruthika Devi received her 5yrs (Integrated course) M.Sc (Information Technology) degree from Vivekanandha Institute of Engineering and Technology for Women , Affiliated to Anna University, Chennai in 2013. She is pursuing her M.Phil (Computer Science) degree Under the Supervision of Dr.R.Manavalan. Her Area of interest is mobile computing.

Dr. R. Manavalan is working as an Associate professor and Head in the Department of Computer Applications. He obtained his Ph.D in Computer Science from Periyar University and published numerous research Papers in International Journals and also presented papers in various National and International Conferences. His Areas of interest are Soft Computing, Image Processing and Analysis, Theory of Computation, Intelligent Computing and Mobile Computing.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY