IJCSE International Journal of Computer Sciences and Engineering Open Access

Case Study Paper Volume-5, Issue-2 E-ISSN: 2347-2693

Identity Based Attack Detection using Spatial Information in Clusters for Wireless Sensor Network

Tuhin Das[1*], Sachin D Choudhari[2]

[1*]Department of Computer Science and Engineering, SBITM (RGPV), Bhopal, India
[2] Department of Computer Science and Engineering, SBITM (RGPV), Bhopal, India

*Corresponding Author: tuhin.subho.das@gmail.com

Available online at: www.ijcseonline.org

Received: 22/Jan/2017 Revised: 30/Jan/2017 Accepted: 17/Feb/2017 Published: 28/Feb/2017

Abstract— **Wireless Sensor Network is a network of wireless devices which is spatially distributed in autonomous tiny computing devices and equipped with sensors, a wireless radio, a processor, and a power source. Wireless sensor networks are deployed in the physical environment to monitor and gather a wide range of information. Due to its dynamic operational and manhandled mobile devices used it also suffers from lot of network security threats. Mostly identity based attacks for example masquerade uses MAC address of some authorized person through malicious device to get hold of the secret information inside the wireless network which largely affects the performance of the network. Identifying a device appropriately is a massive challenge in network securities domain which can be perfectly executed by using the spatial information, a physical property of wireless sensor node. We propose OADL (Optimized Attack Detection & Localization) model which uses the average received signal gain of received signal strength with spatial information correlation to find out the identity of attacker and again using PAM clustering algorithm for detecting the number of with multiple illegitimate identities and eliminate them. When we have the datasets discovered by support vector machines can be used to localize the exact position of multiple illegitimate identities. Evaluating this technique using both wifi (802.11 network) and zigbee model (802.15.4 network) we are able to determine result that attained more than 90% percent hit rate. Using integrated detection and localization algorithms provide high accuracy for multiple attackers.**

***Keywords-** Identity Based Attack, Wireless Sensor Network, Received Signal Strength, Clustering Algorithm, Localization, OADL*

I. INTRODUCTION

A wireless sensor network has powerful sensing, processing, communication ability which helps to observe, measure, process the events and phenomena gathering relevant information on objects. Wireless Sensor network application example as weather monitoring requires data like temperature, barometric pressure etc called as sensing modalities. Various processes associated in wireless sensor applications are categorized into data acquisition network and data distribution network. The openness of the wireless network allows anyone to monitor data transmission over wireless sensor network very easily and from security point of view an adversary can reliably purchase any wireless devices and use them to launch a variety of attacks with ease. Among various types of attacks to break the integrity of the system, identity-based attacks are particularly easy to launch and can create negative impact to network performance. For example, in wifi and zigbee network model, an attacker can gather essential MAC address information during monitoring and revise its MAC address by invoking an ifconfig command to masquerade and generate multiple illegitimate identities. Despite the presence of security techniques in 802.11 including Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), or 802.11i (WPA2), such technique can secure data frames — a spoofing attacker can still cause inevitable impact on the performance of wireless networks. Identity based attacks can cause traffic injection attacks like attack on access control lists, access point attacks and denial of-service (DoS) attacks. Hence it is very essential to get following information:

1) detect the identity based attack in wireless sensor network
2) finding out the number of attackers
3) finding location of multiple adversaries

The conventional method used to avoid address spoofing attack was authentication application. But authentication application requires additional infrastructural overhead and computational power associated with allocating and maintaining cryptographic key [6]. It is difficult to provide authentication for user all the time due to confined power and resources for wireless equipments. In this paper we proceed with a new approach of using the spatial information, a physical property of wireless sensor node to detect the identity based attacks on the wireless network when attackers masquerading as the same node identity hence localizing for multiple adversaries.

We introduce a technique to detect the identity of attacker, find location of multiple adversaries and eliminate them. Our scheme employs the Received Signal Strength (RSS) calculation to implement identity based attack detection and localization over set of access points. By inspecting the average received signal gain of the RSS from each MAC address by the help of clustering algorithm, we have observed that the spatial distance among the access point in signal space is an effective method of testing the identity based spoofing attacks. Partitioning Around Medoids (PAM) is clustering algorithm is used to count the attacker instances. Since we are concerned with attackers who have different locations than valid wireless nodes, utilizing spatial information to express identity based attacks has the unique power to not only recognize the presence of these attacks but also locate adversaries precisely [1][2].This methodology works even when the attacker varies their power levels for transmission to fraud the system of their actual positions and hence they are tracked down successfully.

One major advantage of using spatial information of the sensor node is that it does not involve any additional cost or major modification in the nodes in the wireless network. We analyzing the identity based attack detection in dynamic and robust environments in our course work. The works that are closely correlated to us are [3], [8], [9]. Faria and Cheriton [4] proposed the use of matching rules of signal prints for spoofing detection. Jie Yang et al.[1], Sheng et al. [8] demonstrated the RSS readings and Chen et al. [9] used received signal strength and K-medoids clustering technique to detect identity based attacks.

II. Related Work

The classical approach is the cryptographic system requires good key management and distribution. It is not always easy to implement these kinds of methods due to the fact that it requires infrastructural overhead and cryptographic key management. In the current system, cryptographic technique nodes can be easily attacked which is a critical condition. The wireless nodes are easily accessible and also their memory which can be scanned by the attackers. Cryptographic method only protects the data frames but not the access points. Another aspect of determining security is use of 802.11 or higher protocol which is capable of ensuring data integrity and privacy throughout data transmission. The 802.11 is naive to many attacks at high degree that target to the MAC and its management [5].The three researcher Jie Yang, Yingying Chen and Wade Trappe firstly introduce use of received signal strength (RSS) spatial correlation of wireless nodes to detect the spoofing attacks [1].

Clustering methodology decide the number of attackers involved in the attack. Training data sets are gathered using the SVM (Support Vector Machines) to improve the accuracy of determining the count of attackers [15]. They build the IDOL (integrated detection and localization system that can localize the positions of multiple attackers) [1].

(a) Survey of Received Signal Strength Indicator

Received Signal Strength Indicator (RSSI) is a readily available and cost effective method of localization in wireless sensor networks. RSSI value is measured on the data packets received which act as an indication for replication of node or any physical replacement attacks and also has adept spatial correlation characteristics. Identical physical space provides similar values of RSS readings on the other hand the distinct locations in physical space gives distinct RSS readings. RSS values in array as s[ ] = (s1, s2,...sn) where n indicates the number of benchmark that are observant of the RSS values of the wireless sensor nodes and recognize their locations in network. RSS values reading at the kth benchmark from a wireless sensor node is determined as

$$\mathrm{Sk}\ (d\mathrm{l})\ [d\mathrm{Bm}] = \mathrm{P}\ (d0)\ [d\mathrm{Bm}] - 10\Upsilon \log\ (d\mathrm{l}/d0) + \mathrm{Xk}$$

where P(d0) indicates the power transmission of the node at the distance d0 locally. Υ is the lost path exponent and dl is the shortest distance between node l and the kth benchmark, Xk is the fading of shadow given as input to the system. If the value of RSS does not match in consecutive RSS values, then the node is said to be malicious [1].

(b) Detection of attack by clustering algorithm

Clustering algorithms uses the spatial distance between different instances to measure the similarity among the objects that are closer together although objects from different groups are moved away from each other. RSS-based spatial correlation data is collected from the entire wireless sensor nodes present in the network grid. Accurately, RSS reading from same cluster points in the same time space are grouped together in n-dimensional signal space for the same physical location and for different RSS readings, different clusters are created over time in signal space for different positions. In the condition of identity based attack, the authenticated user and the adversary are using the same ID for data transfer in the network and the RSS readings of that ID is the coalition readings measured from each individual node. We need to perform analysis of clusters on the basis of RSS based spatial correlation to determine the distance in space signal and find out the occurrence of identity based attack in network space. Firstly we use PAM algorithm to define clusters from RSS reading and generate different training data subsets. On the basis of the gained training data subsets the vector for SVM classification is formed and finally, distribution is done using radial SVM for localization of the intrusion.

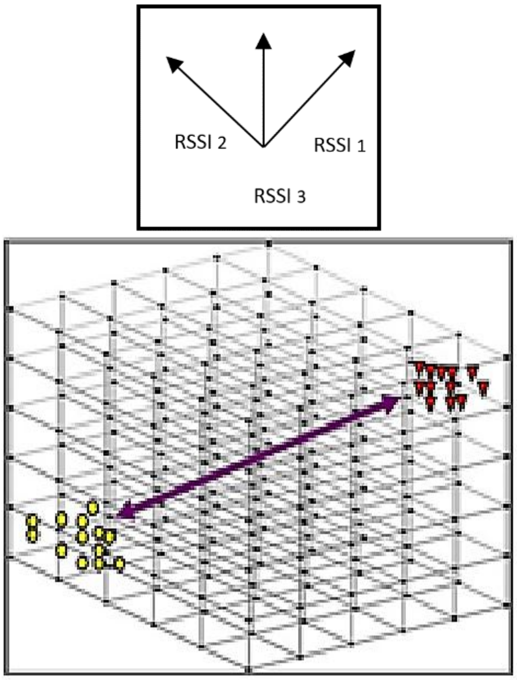


FIG 1: Shows significant different RSS readings from two physical locations

III. Proposed Work

The proposed plan is to overcome the limitations of earlier model so that it works perfectly when the nodes are in both static and dynamic wireless network. An optimized scheme is needed to be developed for fast detection of attacker nodes in the wireless network. The key idea of this scheme is to detect identity based attack in wireless sensor network using Radio frequency Signal Strength [17]. We proposed to create a model called Optimized Attack Detection & Localization (OADL) which can be implemented for detecting identity based spoofing attacks, finding the number of attacker using cluster analysis [14] [16] algorithm depending on RSS based spatial information of sensor nodes and a localization system to identify the location of multiple adversaries even when the sensor nodes have varying power levels for data transmission.

In OADL model the PAM and k means clustering process analysis [16] is used to detect identity based attack and determine the number of attacker. We designed System optimization mechanism for minimum distance span of clusters and improve the accuracy of detecting of the multiple adversaries. If the training data are available, we need to use the Support Vector Machines (SVM) method to enhance and improve the precision of finding the number of attackers [15]. We performed through our experiments for both ZigBee Static and dynamic network. We use NS2 (Network Simulator) for simulation of network, OADL [10] model proved to be highly efficient in identity based attack detection with 90 percent hit rate. Additionally, we can achieve similar localization precision of multiple adversaries.

(a) Optimized Attack Detection & Localization Model
In OADL model, we intent to use RSS readings of each node for cluster analysis for performing attack detection in wireless sensor network. Our paper has following contribution in respective areas.

- To precisely detect the presence of identity based attack
- To find out the number of attackers
- To identify the multiple adversaries even when the sensor nodes have oscillating power levels for data transmission
- To locate the position of multiple attackers in the network
- To provide solution for detecting adversaries in the wireless network with no additional cost or modification to the wireless sensor nodes
- To overcome the conventional approach of key management authentication
- To eliminate overhead from using high configuration network devices

Through OADL model, we can prove that our system is capable of finding spoofing attacks, count the number of attackers, and localize the multiple adversaries [10].
The provisional results are displayed to evaluate the efficiency of our method, especially when attackers are using different transmission power levels.

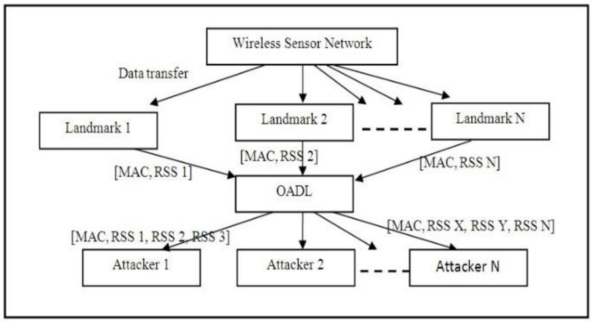


FIG 2: Architecture of OADL model

(b)Identity based Attack Detection
In this [1][2], identity based spoofing Attack detection is discovered. Received Signal Strength (RSS) is a property which is directly associated with positioning of a sensor node in network grid and it is easily available in the wireless sensor network. RSS reading at the ith landmark from a wireless node is given by

$$Si\ (dj)\ [dBm] = P\ (d0)\ [dBm] - 10\Upsilon \log (dj/d0) + Xi$$

where P(d0) indicates the transmitting power of that node at the local distance d0, ϒ the lost path exponent whereas dj is the distance between the wireless sensor node j and the ith landmark, Xi is the shadow fading which is given as input[1].

The nodes having the same transmission power over the static network if its RSS values mismatches with its successive RSS values, then the sensor node is declared to be malicious. The primitive method of finding mean of RSS readings are not capable of differentiating RSS readings from different physical locations hence it is unrealistic for localizing multiple adversaries in dynamic network grid. Distinctive from previous localization process, our optimized detection and localization model implements the RSS medoids retrieved from clustering analysis are used as inputs to localization algorithms to calculate the positions of adversaries in dynamic mobile network. Adversaries are capable of varying the transmission power levels when creating spoofing attacks so that the localization system fails to locate its position precisely.

(c) Handling adversaries using different power levels in data transmission

An adversary can change the data transmission power levels when implementing identity based spoofing attacks so that the localization system is unable to detect its location accurately with the help of algorithms like neigbour discovering algorithm. Jie Yang, Yingying (Jennifer) Chen and Wade Trappe[1] proposed the loss pass equation that uses received power as function of the distance to node and landmark is given below:

$$P(d)[dBm] = P(d0)[dBm] - 10\Upsilon\log10(d/d0)$$

where *d* is the distance indicator between the transmitting node and the landmark, P(*d0*) indicates the transmission power of sensor node at the local distance *d0,* and Υ is the lost path exponent. We can state the difference between the received power of two landmarks i and landmark j as

$$P(di) – P(dj) = 10\Upsilon i\log10(di/do) -10\Upsilon j\log10(dj/do)$$

(d) Localization

The Localization system determines how the information concerning positions and distances managed in order to allow all the nodes of a wireless network to locate their respective positions in the network grid. To calculate the performance of OADL model for localizing multiple adversaries, we have representative localization algorithms as nearest neighbour matching in signal space [13]. Given with set of experimented RSS reading with an unknown position in the network grid, nearest neighbour node searches the x, y coordinate of the nearest neighbour in the signal map to localize the sensor node, while “nearest node” is described as the euclidean distance of received signal strength readings of that node in N-dimensional network signal space, where N is the count of access points in the wireless network. In this block, we have used 30 nodes that are estimating the neighbour nodes with their data transmission range over the network with the help of landmarks. Then it gives its position to all of its neighbours. It occurs with all the nodes at regular intervals of time. And last it determines the location of malicious node in 2 dimensional space [18].

IV. SYSTEM IMPLEMENTATION

(a) Simulation Environment

For network simulation purpose, we proposed to use the latest version of NS-2, network simulator is a name for series of distinct network simulators, like NS-1, NS-2 and NS-3. All of these are network simulator, mostly used in research, education, training and teaching. NS-2 is open source publicly available free software under the GNU GPLv2 license for research, development, and training.

(b) Simulation Parameter

We have to set number of parameters for simulation according to network model used [19]. There are number of simulation parameters which can be varied, change in value of different performance metrics, which are displayed in table below.

Parameter	Value
Simulator	NS-2 (Version 2.35)
Channel type	Channel/Wireless
Radio propagation model	Propagation/Two ray ground
Network interface type	Phy/WirelessPhy/ 802_15_4
Interface queueType	Queue/DropTail/ PriQueue
Traffic Type	CBR
Antenna	Antenna/ Omni Antenna
Maximum packet	100
Area (M*M)	1000*1100
Simulation Time	30 seconds
No of Nodes	28
Routing Protocol	AODV Performance

Performance of OADL model in wireless network can be seen by running the simulation, the figure 3. Shows the output of wireless adhoc network (ZigBee 802.15.4) there are 30 node in the network grid which is set in 1000*1100m, and each moving randomly and each sensor node is capable of data transmission and creating network. Optimized Attack detection and Localization model demonstrates the random number of landmark are used to launch the data transmission and evaluating the RSS reading for each neighbouring nodes then it returns the number of malicious node in network and location of that sensor node.

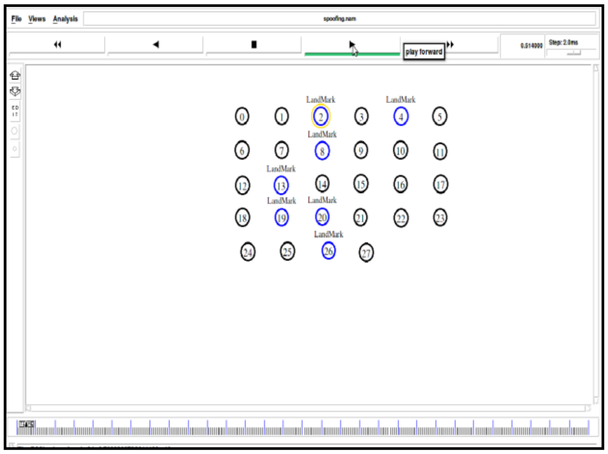


FIG 3: Ns2 Simulation Result showing the selection of landmark nodes

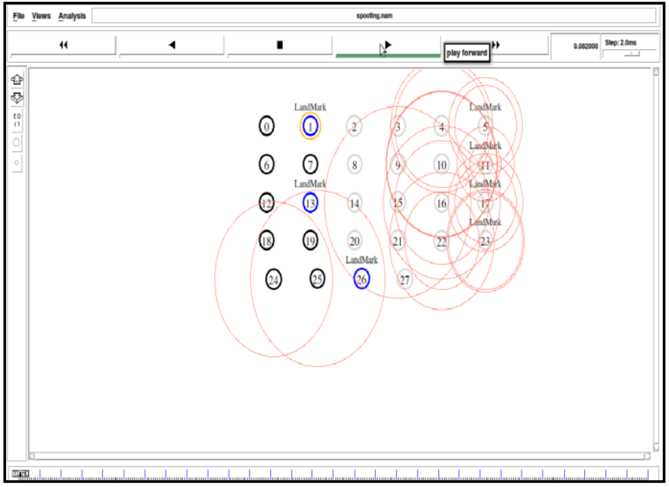
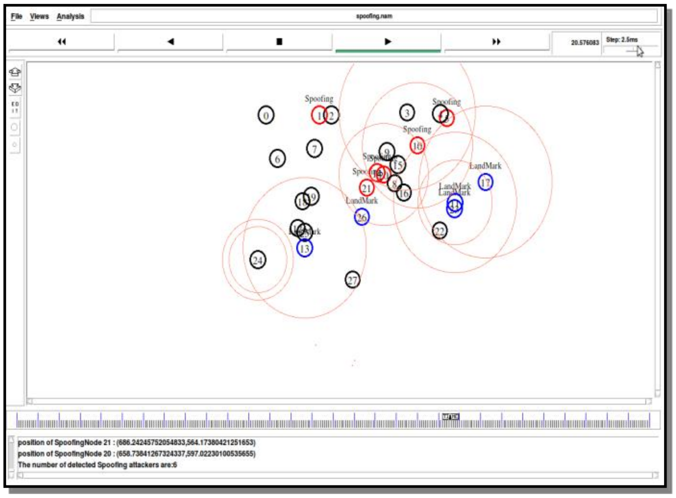
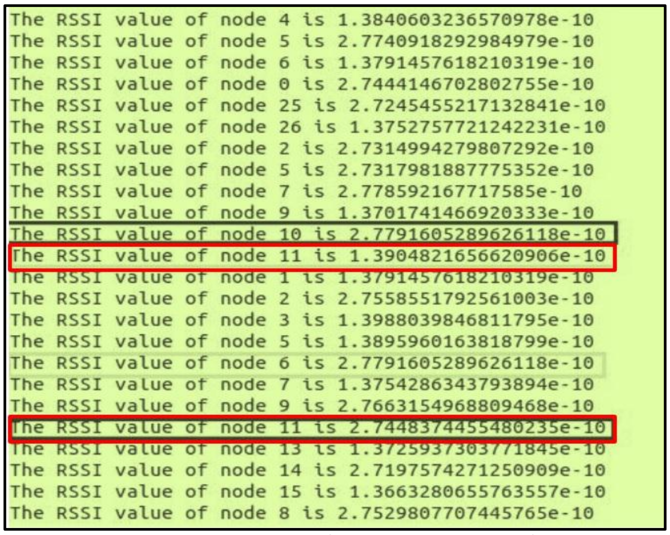


FIG 4: Ns2 Simulation Result showing calculation of RSSI value from different nodes.



```
position of SpoofingNode 21 : (686.24245752054833,564.17380421251653)
position of SpoofingNode 20 : (658.73841267324337,597.02230100535655)
The number of detected Spoofing attackers are:6
```

FIG 5: Ns2 Simulation Result for detection the spoofing nodes



```
The RSSI value of node 4 is 1.3840603236570978e-10
The RSSI value of node 5 is 2.7740918292984979e-10
The RSSI value of node 6 is 1.3791457618210319e-10
The RSSI value of node 0 is 2.7444146702802755e-10
The RSSI value of node 25 is 2.7245455217132841e-10
The RSSI value of node 26 is 1.3752757721242231e-10
The RSSI value of node 2 is 2.7314994279807292e-10
The RSSI value of node 5 is 2.7317981887775352e-10
The RSSI value of node 7 is 2.778592167717585e-10
The RSSI value of node 9 is 1.3701741466920333e-10
The RSSI value of node 10 is 2.7791605289626118e-10
The RSSI value of node 11 is 1.3904821656620906e-10
The RSSI value of node 1 is 1.3791457618210319e-10
The RSSI value of node 2 is 2.7558551792561003e-10
The RSSI value of node 3 is 1.3988039846811795e-10
The RSSI value of node 5 is 1.3895960163818799e-10
The RSSI value of node 6 is 2.7791605289626118e-10
The RSSI value of node 7 is 1.3754286343793894e-10
The RSSI value of node 9 is 2.7663154968809468e-10
The RSSI value of node 11 is 2.7448374455480235e-10
The RSSI value of node 13 is 1.3725937303771845e-10
The RSSI value of node 14 is 2.7197574271250909e-10
The RSSI value of node 15 is 1.3663280655763557e-10
The RSSI value of node 8 is 2.7529807707445765e-10
```

FIG 6: Detection the spoofing nodes by the help of RSSI values

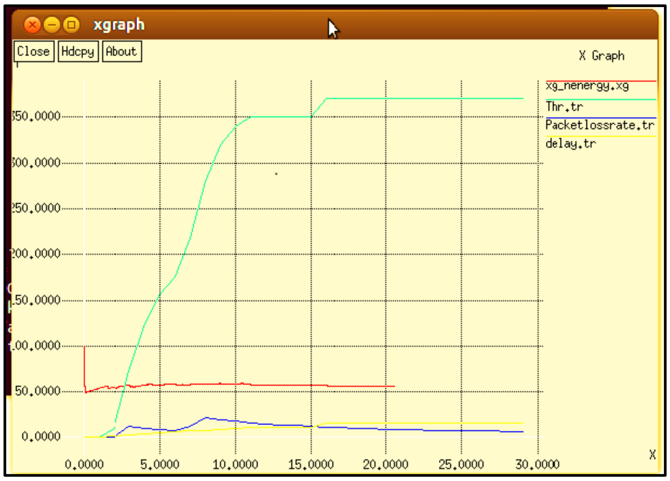


FIG 7: Throughput, Packet loss rate, end to end delay & energy graph Of OADLM

From the graph showing throughput, packet loss rate, end to end delay and energy graph we can say that value of throughput is increasing apparently from starting for network as well as PDR values for System is constant and low as the time passes. Thus we can find loss of energy and packet loss is reduced throughout the simulation that indicates network providing high performance.

V. CONCLUSION

In this approach we propose to use OADL (Optimized Attack Detection & Localization) model which uses the average received signal gain of received signal strength with spatial information correlation associated with every wireless devices as the base idea for detection of identity based spoofing attacks in a wireless network. We are able to draw theoretical analysis on data gathered after the whole demonstration that cluster analysis based on RSS readings can detect presence of spoofers and can also determine exact count of adversaries with their location and eliminating them efficiently. We have deployed and experimented this OADL model in both 802.11 and 802.15 network beds and found that our detection mechanism is highly efficient with more than 90 percent detection rate.

REFERENCES

[1] Yingying Chen, J. Cheng, W. Trappe, Jie Yang, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", IEEE Transactions on Parallel & Distributed Systems (IEEE TPDS), Volume 24, No.1, Pages 44-58, 2013.

[2] Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", Proc. USENIX Security Symp., at San Diego, USA pp. 15- 28, August 2003.

[3] D.G.Harkut, M. S.Ali and P.B.Lohiya, "Scheduling Task of Wireless Sensor Network Using Earliest Deadline First Algorithm", International Journal of Scientific Research in Computer Science and Engineering, Vol.2(2), pp.1-6, Apr 2014

[4] Kaur H. and Kaur B, "Selective DDoS Attacks in Application server and Wireless Network – Survey", International Journal of Computer Sciences and Engineering, Vol.4(8), pp.78-80, Aug -2016

[5] Q. Li, W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON) at Reston, Virginia, USA, September 2006. ISBN: 1-4244-0626-9.

[6] A. Singh, L.Kaur and K. Singh, "Impact of DDoS Attacks on Different Services Using Various AQM Techniques", International Journal of Computer Sciences and Engineering, Vo.4(4), pp.149-155, Apr -2016

[7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A.Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," Proc. IEEE INFOCOM at Phoenix, Arizona, USA, Apr. 2008. ISBN: 978-1-4244-2219-7.

[8] Y. Chen, W. Trappe and R. P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, San Diego, CA, pp. 193-202, 2007. ISBN: 1-4244-1268-4.

[9] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking at San Francisco, CA, USA, pp. 116-127, 2008. ISBN: 978-1-60558-096-8

[10] Das T "Identity Based Attack Detection and Localization by the Clustering in Wireless Sensor Network" International Journal of Computer Sciences and Engineering, Vol.-4(2), pp.96-99, Feb 2016. E-ISSN: 2347-2693

[11] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE INFOCOM, Tel Aviv, Israel, pp. 775-784 2000. ISBN: 0-7803-5880-5.

[12] J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," Proc. Fourth Int'l Workshop System Management Techniques, Processes and
Services (SMTPS), Miami, Florida USA, pp. 1-6, Apr. 2008.

[13] 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.

[14] ma Korupolu, S Kartik and G Kalyan Chakravarthi, "An Efficient Approach for Secure Data Aggregation Method in Wireless Sensor Networks with the impact of Collusion Attacks", International Journal of Scientific Research in Computer Science and Engineering, Vol.4(3), pp.25-28, Jun 2016.

[15] N. Cristianini and J. Shawe-Taylor, "An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods" Cambridge University Press, NY, USA pp. 1360142, 2000. ISBN 0-521-78019-5.

[16] L. Kaufman and P.J. Rousseeuw, "Finding Groups in Data: An Introduction to Cluster Analysis", Wiley Series in Probability and Statistics, New York, USA, pp. 131-146, 1990. ISBN: 9780471878766.

[17]P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system", Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Tel Aviv, Israel, pp. 775-784, 2000. ISBN: 0-7803-5880-5

[18] Barapatre M "Spoofing Attack Detection and Localization inAdhoc network using Received Signal Strength (RSS) " International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, pp.6706-6710, May 2014. ISSN: 2278-1021.

[19] M. Bohge and W. Trappe, "An Authentication Framework For Hierarchical Ad Hoc Sensor Networks," In Proc. ACM Workshop on Wireless Security (WiSe) San Diego, CA, USA, pp. 79–87, 2003. ISBN: 1-58113-769-9

AUTHOR'S PROFILE

Tuhin Das, is a final year student of M.Tech in CSE from SBITM College, under RGPV, Bhopal. His areas of interest are Wireless Sensor Network, Java, Network Security, and Data Mining.

Sachin D Choudhari, is a faculty in computer science department in SBITM College, under RGPV Bhopal. His areas of interest are Wireless Sensor Network, cloud computing, Network Security, Digital Image Processing and Data Mining