iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 Issue: IV Month of publication: April 2015

DOI:

www.ijraset.com

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

Volume 3 Issue IV, April 2015
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

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

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

Abstract*--Wireless spoofing attacks are easy to launch, it plays a significant role in the performance of wireless sensor networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. The challenging tasks in Wireless Sensor Network are identification of spoofing attackers, determination of number of attackers, localization of multiple adversaries and eliminating them. The clustering approach is used to detect the spoofing attackers and localize them. This approach fails to predict the attackers accurately. To overcome this problem, this paper proposes Intrusion Detection System (IDS) to detect the spoofing attackers. The cluster head act, as IDS to monitor the behavior of nodes in their cluster such as packet transmission which helps to identify the misbehaving nodes in wireless sensor network. The simulation result clearly shows that the proposed scheme detects the spoofing attackers in Wireless Sensor Network efficiently and robustly.

Keywords: Wireless network security, spoofing attack, attack detection localization, Intrusion Detection System

I. INTRODUCTION

Wireless sensor network is a network of simple sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Wireless networks are usually deployed in an unattended manner and are controlled remotely by the network operator [1]. 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 [2].

Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. 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 [24]. Among various types of attacks, spoofing attacks are easy to launch that degrades the network performance highly. Spoofing is when an attacker pretends to be someone else in order to gain access to restricted resources or steal information. 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 to address potential spoofing attacks based on cryptographic schemes [3], [4]. 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 are not relevant on cryptography for detecting spoofing attacks. Attackers who have different locations then the legitimate wireless nodes are concerned, spatial information is used not only to identify the presence of spoofing attacks but also to localize adversaries [6][25]. Spatial correlation is employed to detect spoofing attacks in wireless sensor network without any additional cost or modification. The overview of the proposed model is discussed in section 1.1.

A. Overview Of Proposed Model

Fig.1 shows the overview of the proposed model. The nodes information in the cluster is collected by cluster head which acts as Intrusion Detection System (IDS) for monitoring the cluster member. If the IDS find the attacker, it passes the alarm message to the source node which eliminates the attacker. The K-Means clustering approach and Intrusion Detection System mechanism are implemented to determine the number of spoofing attacks and localize the same in wireless sensor network.

©IJRASET 2015: All Rights are Reserved

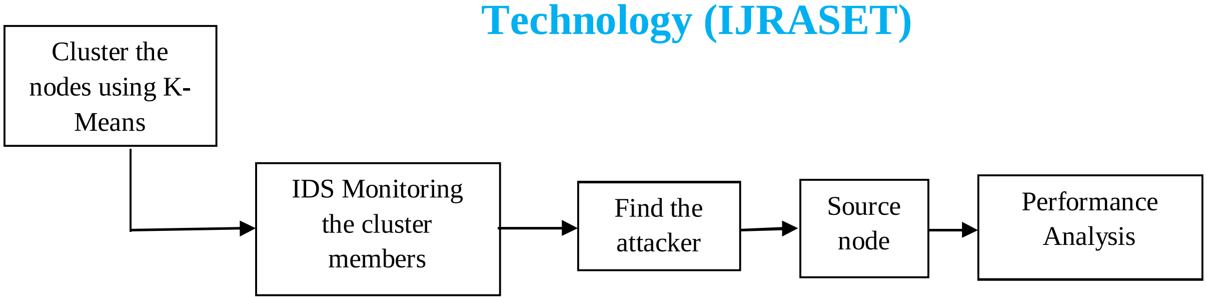

Cluster the nodes using K-Means
IDS Monitoring the cluster members
Find the attacker
Source node
Performance Analysis

Figure 1. Block diagram of proposed system

The rest of this paper is organized as follows: In Section II, some related works are discussed. Section III discusses the Dynamic Source Routing Protocol. Ad hoc On demand multipath Distance Vector (AOMDV) is discussed in Section IV, the enhanced framework for detecting and localizing the spoofing attack is provided in section V. In Section VI, the performance analysis of the proposed framework is discussed. Section VII provides the conclusion with future scope.

II. RELATED WORK

To prevent spoofing attacks, cryptographic based authentication is used traditionally. Wu et al. [5] have introduced a Secure and Efficient Key Management (SEKM) framework. SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. Wool [7] 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 thus to detect spoofing attacks in wireless networks [8]. Kihong Park and Heejo Lee [9] proposed the concept of Probabilistic Packet Marking (PPM) for tracing the source (i.e.) origin of DoS attack. P. Bahl and V.N. Padmanabhan [10] proposed and demonstrated the method of RADAR for identifying the location of attacker in wireless sensor network. T.Roos et al., [11] 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.

Bellardo and S. Savage [12] conducted an experiment for identification of the attacks by using efficacy and potential low-overhead implementation to mitigate the underlying vulnerabilities. Ping Tao et al., [13] proposed a technique named Traditional localization for increasing robustness. Malicious nodes can easily violate the assumptions by modulating their transmission power of each packet.

Yingying Chen et al., [14] proposed two approaches K-means cluster analysis and Area-based or Point-based Localization algorithms for wireless spoofing attack. Qing Li and Wade Trappe [15] presented a non cryptographic mechanism for detecting device spoofing on a wireless network. Shang.L and Arora.A [16] 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. V.Shyamaladevi and Dr.R.S.D. WahidaBanu proposed the Stack Path identification marking technique and filtering mechanism [17].

C. Hsu and C. Lin [18] 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 [19] proposed the mobility-aware access control mechanism which is more suitable for both wireless and wired environments.

III. DYNAMIC SOURCE ROUTING PROTOCOL

DSR is a reactive routing protocol i.e. it determines the proper route only when packet needs to be forwarded. For restricting the bandwidth, the process finds a path when a path is required by a node (On-Demand Routing). In DSR, the sender (source, initiator) determines the whole path from the source to the destination node (Source-Routing) and deposits the address of the intermediate nodes of the route in the packets. DSR is beacon-less, which means there are no hello-messages used between the nodes to notify their neighbors about their presence. DSR is based on the Link-State Algorithms which means each node is capable to save the best way to a destination. If any change appears in the network topology, then the whole network will get this information by flooding. The DSR protocol is composed of two main mechanisms, that work together to allow discovery and maintenance of source routes which are Route Discovery and Route Maintenance. The disadvantage of DSR is when the packet size increases then the

©IJRASET 2015: All Rights are Reserved

performance gets degraded. So AOMDV protocol is considered for this research work.

IV. AD HOC ON DEMAND MULTIPATH DISTANCE VECTOR (AOMDV)

AOMDV is a multi-path routing protocol. It is an extension of AODV and also provides two main services. They are route discovery and maintenance. Unlike AODV, every RREP is being considered by the source node and multiple paths are discovered in one route discovery. Being the hop-by-hop routing protocol, the intermediate node maintains multiple path entries in their respective routing table. As an optimization measure, by default the difference between primary and an alternate path is equal to 1 hop. The route entry table at each node also contains a list of next hop along with the corresponding hop counts. Every node maintains an advertised hop count for the destination. Advertised hop count is defined as the “Maximum hop count for all the paths”. Route advertisements of the destination are sent using this hop count. An alternate path to the destination is accepted by a node if the hop count is less than the advertised hop count for the destination. AOMDV can be applied even in the presence of unidirectional links with additional techniques to discover bidirectional paths in such scenarios [22].

In AOMDV, route discovery procedure finds routes on demand. RREQ is propagated from the source towards the destination that establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths to form multiple forward paths to the destination of the source and intermediate nodes. Note that AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency [23]. The core of the AOMDV protocol lies in ensuring that multiple paths discovered are loop-free and disjoint, and are efficient in finding such paths using a flood-based route discovery. AOMDV route update rules, applied locally at each node, play a key role in maintaining loop-freedom and disjointness properties. The AOMDV define three types of control message for route maintenance: RREQ, RREP and RERR.

RREQ: a route request message is transmitted by a route required node.

RREP: a route reply message is unicast back to the originators of a RREQ.

RERR: route error message is used to notify other nodes for the loss of the link.

For example consider the situation in Figure 2, where a RREQ packet propagates along S-A-X-D (that will be our primary path) and along S-A-Y-D. Suppose RREQ packet arrives to Y from B but Y has already processed the RREQ packet from A. In this way Y propagates the RREQ packet from A but it records the entry of B. When the RREQ packet arrives to the destination, D sends a RREP packet along X and Y. Y has two entries for S, A and B. The first entry recorded from Y is A. Therefore Y will send the RREP packet to A. In the original AOMDV, node A maintains the entry for node Y (in the forward path) and in this way node Y thinks that its RREP packet arrived correctly to the source S through a link-disjoint path. In this way if there is a link breakage A-S or X-D the “alternate” path S-A-Y-D can be used when it is yet active, but this does not respect the property of link-disjointness. AOMDV can be used to find node-disjoint or link-disjoint routes.

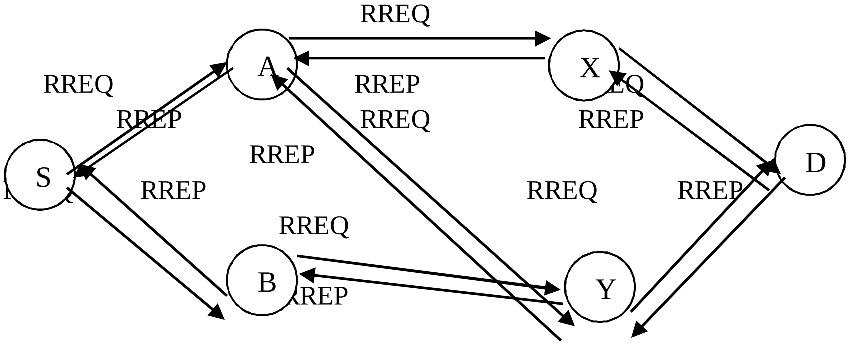


Figure 2: AOMDV protocol working

The Advantage of AOMDV is Loop free, loops are overcome by using sequence number and AOMDV is Disjoint. The advantage of using AOMDV is that it allows intermediate nodes to reply for RREQs, while still selecting disjoint paths. But, AOMDV has more message overheads during route discovery due to increased flooding and since it is a multipath routing protocol, the destination replies to the multiple RREQs whose results are in longer overhead. Three mechanisms are used in AOMDV protocol. They are Route Discovery, Route Reply and Route maintenance

The AOMDV has two main components:

Route update rule to establish and maintain multiple loop free paths at each node.

©IJRASET 2015: All Rights are Reserved

A distributed protocol to find link disjoint paths.

V. K-MEANS APPROACH USING RECEIVED SIGNAL STRENGTH (RSS)

Received signal strength is measured across a set of access point to carry out the spoofing detection and localization. The Received Signal Strength (RSS) is a measurement that is hard to falsify randomly and it is highly associated to the transmitter's location**.** RSS is the signal strength of a received frame measured at the receiver's antenna. Many commercial 802.11 networks present per-frame RSS measurements. RSS is interrelated to the transmission power, the distance between the transmitter and the receiver, and the radio location because of multi-path and inclusion effects. Further, the attacker is from its victim, the more possibility in the variation of RSS pattern extensively and the easier to detect the spoofing attacks. In GADE method, K-Means Method is used to perform clustering analysis in RSS.

The RSS-based spatial correlation is inherited from wireless nodes for spoofing attack detection. The RSS readings from a wireless node may fluctuate and cluster together. The RSS readings over time from the same physical location that 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 use 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 μ_0 : 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    : The location information from all the nodes and assign the centroid.
OUTPUT:  Cluster the nodes

Step 1: Assign each node 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 close 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 Step 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

A. Intrusion Detection System (Ids)

Intrusion detection is a set of actions that determine and report unauthorized activities in wireless sensor network. It detects the violation of confidentiality, integrity and availability. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The threats that damage the security in WSN can be detected by the Intrusion detection systems (IDSs). IDS had an ability to identify the network intrusions and misuse by gathering and analyzing data. The wireless IDS can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations in WSN. Thus it is desirable to monitor the attacks and report the same to a source node to avoid losing an important event.

Fig 3, shows that the group of nodes forms a cluster and a cluster head act as an Intrusion Detection System (IDS). The Control Authenticator (CA) distributes the public key and private (secrete) key to each node in the cluster. The IDS monitor the activities of all the nodes in the cluster. The source node S starts to send the packets to their destination node D. Based on the public key the IDS monitor each and every activity of the nodes in the cluster such as transmission power and energy level. At the time of packet sending the sender node check the receivers secrete key of the receiver. If there is any change in the transmission power or the secret is not matched then IDS consider it as an attacker. Before the packet is dropped by the attacker the IDS send the alarm message to the source node and also all the nodes in the network. The source node gets the information from the IDS and takes the re-routing to reach the destination using the AOMDV routing protocol. This mechanism decrease the packet drop and increase the throughput and packet delivery ratio.

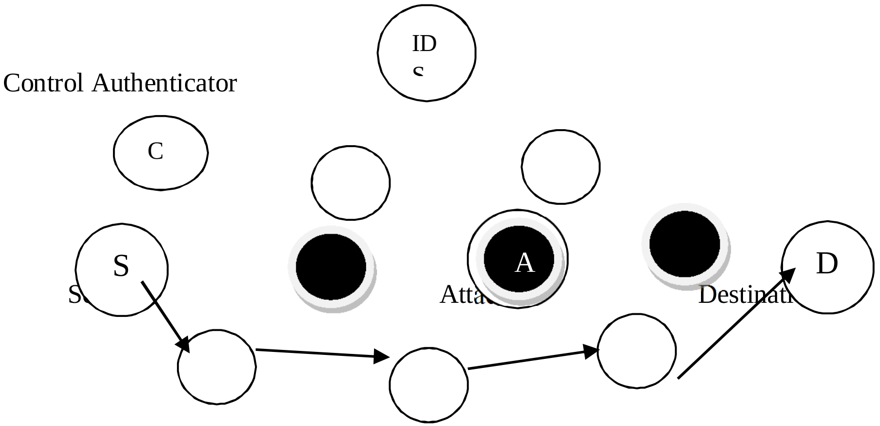


Figure 3: Working of IDS

There are two types of detection techniques: signature detection and anomaly detection. IDS with signature compare the current activity of the nodes with the stored attack profiles and generate an alarm based on the profile. The anomaly IDS compares the systems normal profile with the current activity in the other method. Basically the major security challenges in wireless sensor networks are (i). the size of sensors (ii) consequent the processing power, (iii) memory and (iv) type of tasks expected from the sensors. Of course today's IDS technology offers some automation like notifying the administrator in case of detection of a malicious activity, shunning the malicious connection for a configurable period of time, dynamically modifying a router's access control list in order to stop a malicious connection etc. But it is still very important to monitor the IDS logs regularly to stay on top of the occurrence of events. In this algorithm, firstly create IDS node in which the AOMDV is set as a routing protocol. Then after the creation, the IDS node check the network configuration and capture lode by finding that if any node is in its radio range and also the next hop is not null, then capture all the information of nodes.

With the help of this information IDS node creates a normal profile which contains information like type of packet, in our case (protocol is AOMDV, packet type TCP, UDP), time of packet send and receive and threshold. After creating normal profile the threshold checking is done in the network i.e. if network load is smaller than or equal to maximum limit and new profile is smaller than or equal to maximum threshold and then there is no attack. If there is an attack in the network, find the attack. For this process it compares normal profile with each new trace value i.e. check packet type, count unknown packet type, arrival time of packet, sender of packet, receiver of packet. And after detection of any anomaly in that parameters then block that packet sender node (attacker node). The IDS mechanism for attack detection in wireless sensor network is given in Figure 4.

```
IDS Mechanism for detection and Localization in WSN
Input   : A topology in which m number of malicious node present in a set of n number of sensor
          nodes.
Output: Set of clusters which are having IDS as a header used to find malicious nodes. Set initial
          parameter of network
```

©IJRASET 2015: All Rights are Reserved

```
Step 1: Create node =IDS;
              Set routing = AOMDV;
Step 2: If ((node in radio range) && (next hop! =Null)
              { Capture load (all_node)
Step 3: Create normal_profile (rreq, rrep, tsend, trecv, tdrop)
             { Time;
              Tsend, trecv, tdrop, rrep, rreq
             }
             Threshold_parameter ()
Step 4: If ((load<=max_limit) && (new_profile<=max_threshold) &&
               (new_profile>=min_threshold))
               { No any attack; }
               Else {
              Attack in network;
Step 5: Find_attack_info ();
              }
              Else {
             "Node out of range or destination unreachable" }
Step 6: Find_attack_info ()
               {
Step 7: Compare normal_profile into each trace value
Step 8: If (normal_profile! = new trace_value)
             { Check pkt_type;
              Count unknown pkt_type;
             Arrival time;
             Sender_node;
             Receiver_node;
Step 9: Block_Sender_node(); //sender node as attacker
             }
```

Figure 4: IDS for attack detection in WSN

VI. EXPERIMENTAL ANALYSIS

Simulations are conducted to analyze the performance of proposed Intrusion Detection System (IDS) for spoofing attack detection. The replication surroundings are produced using NS-2 for WSN. NS2 came as extension of Tool Command Language (TCL). The execution of NS-2 is carried out by means of cluster environment of 50 wireless mobile nodes. The simulation area or open area topology of NS-2 execution is 1200 meters x 1200 meters. Simulation path is used to indicate the source to destination connections.

Table 1. NS-2 Simulation Configuration Settings

Parameters	Value
Version	Ns-allinone 2.35
Number of Nodes	50
Simulation Area	1200m x 1200m
Broadcast Area	250 m
Data size	512 bytes
Simulation Time	360 sec
MAC Protocol	IEEE 802.11
Routing Protocol	AOMDV

©IJRASET 2015: All Rights are Reserved

NS-2 is used to build non real time wireless environment at low cost. The parameters and their values used for simulation configuration settings are tabulated in Table 1. The performance of the proposed method is analyzed using the evaluation metrics such as Throughput, Packet Delivery Ratio and Packet Drop Rate. The shortest descriptions of these parameters are discussed below. The amount of data transferred in a given amount of time from source to destination is called throughput. The network performance is good when the throughput and packet delivery ratio is high and packet drop is low. Throughput is defined as

$$\textbf{Throughput} = \frac{P}{T}$$

where P is Total number of received Packets and T is Transmission Time.

Table 2: Throughput

Time (ms)	Throughput	
	K-Means	IDS
12	9	21
15	15	35
18	26	44
21	52	64
24	75	83

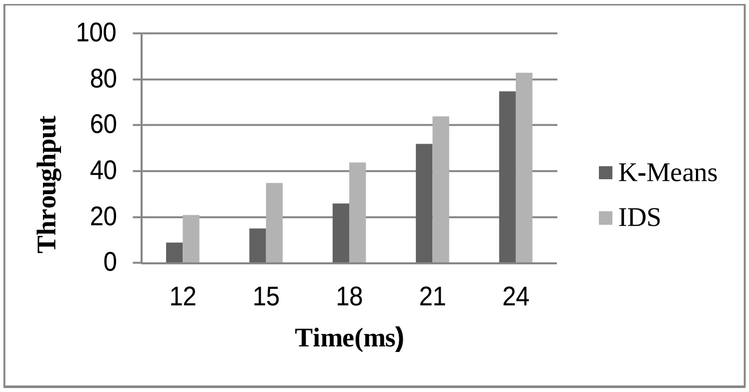


Figure 5: Throughput comparison between K-Means and IDS mechanism

The simulation results showed that the IDS achieve the high throughput than the K-Means approach. The results in table 3 show the throughput earned by the Intrusion Detection System and the K–means approach and the same is flashed in fig 5. In the time duration of 12 milliseconds, the throughput earned by the K-Means approach is 9% where as the IDS achieves 21% which is 10% higher than the K-Means approach.

The packet Delivery Ratio (PDR) refers to the ratio of packets transmitted and received from the source to destination successfully over the network. The PDR ratio is measured in the percentage as

$$\text{PDR} = \frac{P_r}{P_s} \times 100$$

where P_r is the received packets and P_s is the send packets.

Table 3: Packet Delivery Ratio

Time (ms)	Packet Delivery Ratio	
	K-Means	IDS
12	15	27
15	32	45
18	54	65
21	68	82
24	81	95

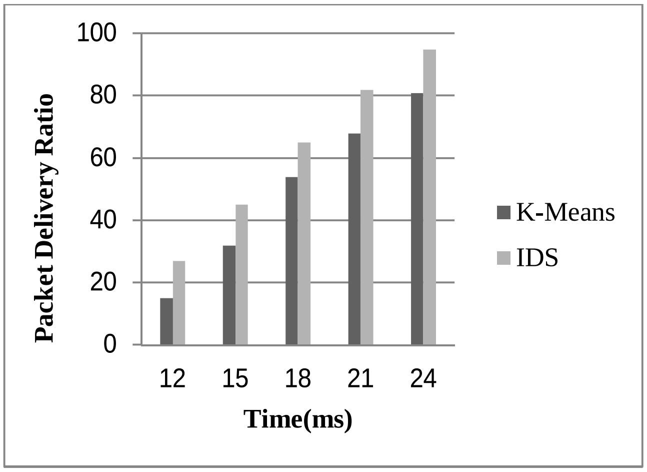


Figure 6: PDR comparison between K-Means and IDS mechanism

Packet Delivery Ratio is the ratio between sum of total number of packets received by destination and sum of total number of packets sent by source. The simulation results clearly show that Packet Delivery Ratio value will be low in transmission time by 12 milliseconds. Packet Delivery Ratio (PDR) values are increased while the transmission time increases from 12 milliseconds to 24 milliseconds for both K-Mean approach and Intrusion Detection System (IDS). The results in table 4, show the Packet Delivery Ratio of IDS and the K–means clustering approach and the same is projected in fig 6. The approach which yields high Packet Delivery Ratio is considered as better attack detector approach. While comparing K-Mean approach with IDS, the IDS yield highest Packet Delivery Ratio. From this study, reliability of IDS is better than K-Mean approach and it is noted that IDS approach is efficient than the other approach.

Packet Drop Rate is the differences between numbers of packets send by the source and number of packets received by the destination respectively. It is used to know the percentages of Packets Drop during the packet transmission from source to destination. The pocket Drop is defined as

Pocket Drop Rate = (No. of Packet Sent – No. of Packet Received)

©IJRASET 2015: All Rights are Reserved

Table 4: Packet Drop Rate

Time (ms)	Packet Drop Rate	
	K-Means	IDS
12	0.2	0
15	0.4	0
18	0.5	0.1
21	0.7	0.1
24	0.7	0.1

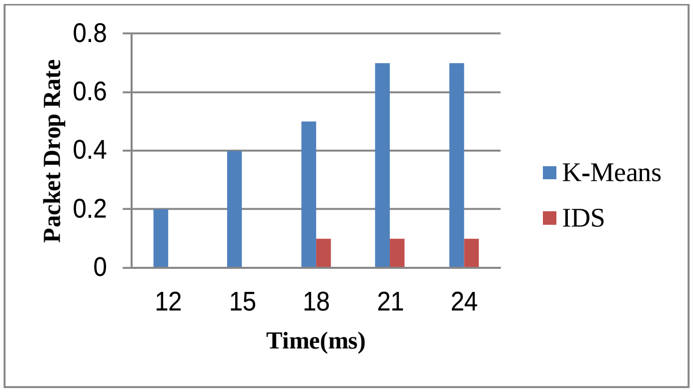


Figure 7: Packet Drop Rate comparison between K-Means and IDS mechanism

The Packet Drop Rate achieved by the methods K-Mean and Intrusion Detection System for various time slots are provided in the table 5 and the same is flashed in the Fig 7. The percentage of the Packet Drop Rate is defined as number of packets dropped is divided by the total number of packets sent. From the simulation result, it is noted that the less packet drop rate is achieved by the IDS than the K-Means approach. The Packet Drop Rate achieved by the K-Means in the time duration of 24 milliseconds is 0.7% where as the IDS achieves less packet drop rate of 0.1% which is 0.6% lower than the K-Means approach.

VII. CONCLUSION

In this paper, the spoofing attack detection and localization scheme such as K-Means and Intrusion Detection System (IDS) are analyzed in Wireless Sensor Network using NS2 simulator. The K-Means approach with Received Signal Strength (RSS) is performed to detect the spoofing attackers in wireless sensor network. The Intrusion Detection System (IDS) with AOMDV is proposed to detect the spoofing attack. The simulation results showed that the performance of the IDS with AOMDV is better for efficient data transmission from sender to receiver by updating the next shortest path. In the future, a reliable and energy-efficient trust mechanism can be designed for identifying the attackers in WSNs to facilitate high result than the other.

REFERENCES

[1] S. Capkun and J.P. Hubaux. Secure positioning in wireless networks. IEEE Journal on Selected Areas in Communications, 24(2):221–232, February 2006.

[2] 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.

[3] Q. Li and W. Trappe, “Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks,” in Proc. IEEE SECON, 2006.

©IJRASET 2015: All Rights are Reserved

[4] Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in Proc. IEEE IPDPS, 2005.

[5] 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.

[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] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

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

[19] 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.

[20] Shaily Mittal Prabhjot Kaur “Performance comparison of AODV, DSR and ZRP Routing Protocols in Manets” International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009.

[21] J. Liu, J. Chen, and Y. Kuo, “Multipath routing protocol for networks lifetime maximization in ad-hoc networks,” Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom '09), 2009.

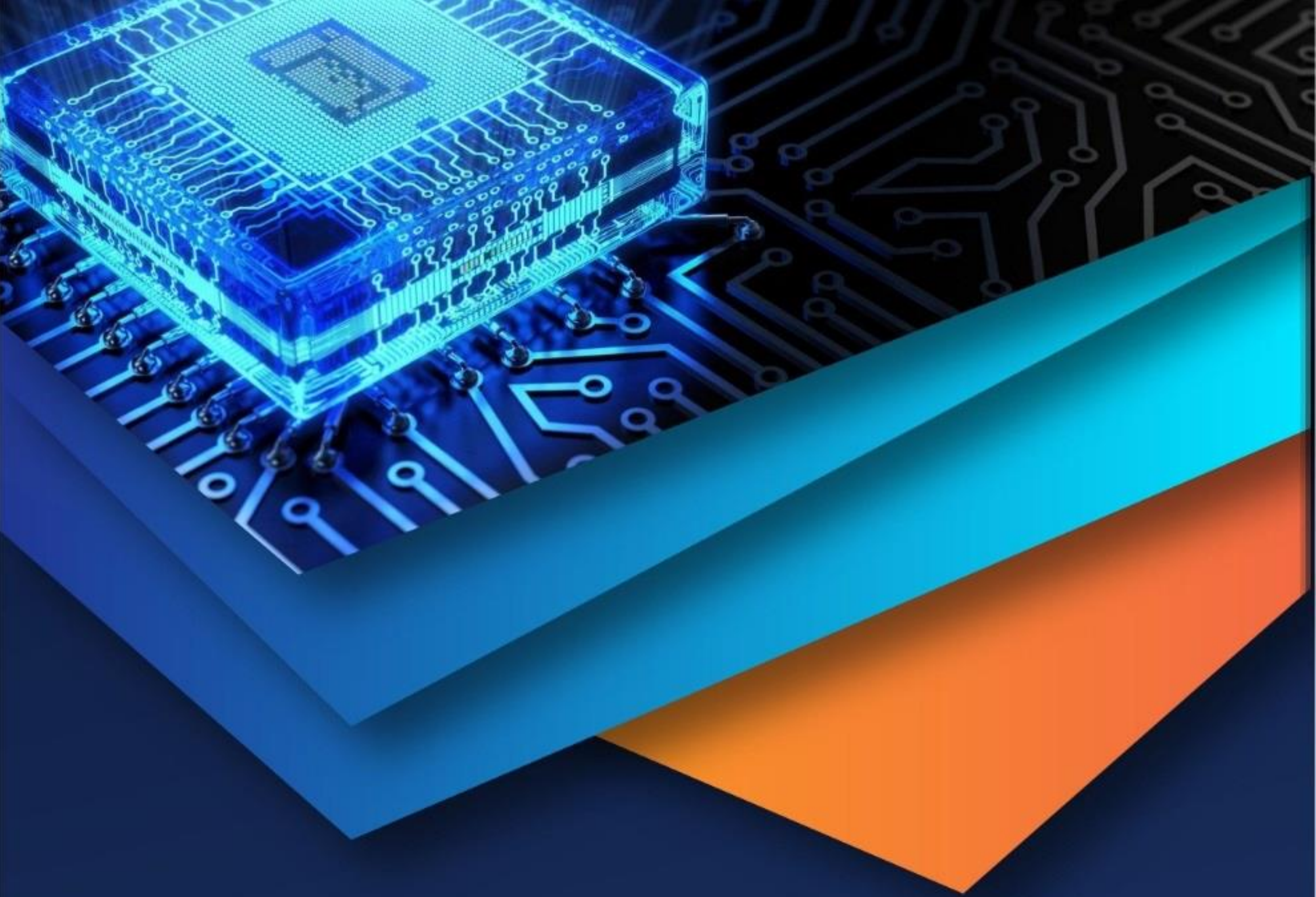
[22] N. Meghanathan, “Stability-energy consumption tradeoff among mobile ad hoc network routing protocols,” Proc. Third Int’l Conf. Wireless and Mobile Comm. (ICWMC ’07), Mar. 2007.

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

[24] 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.

[25] Yang Gao, Hong Li, Mingquan Lu, and Zhenming Fen, “Intermediate Spoofing Strategies and Countermeasures”, Tsinghua Science And Technology, ISSN ll 1007-0214 ll 06/10 ll pp599-605, Volume 18, Number 6, December 2013.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)