Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 2, February 2015, pg.92 – 103

RESEARCH ARTICLE

WATCHDOG MECHANISM FOR PREVENTING MULTIPLE SPOOFING ATTACKERS IN WIRELESS NETWORKS

P.Kiruthika Devi[1], Dr. R.Manavalan[2]
Research Scholar in Department of Computer Science[1], Head of the Department of Computer Applications[2]
K.S.Rangasamy College of Arts and Science, Tiruchengode-637-215, India
Email: *kirthi.bala90@gmail.com*

Abstract-- Spoofing attack is an identity based attack through which one can successfully masquerade the ID of other 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 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 dissertation proposes Watchdog mechanism to detect the spoofing attackers. The watchdog monitoring mechanism monitors and records its neighbors' behaviors such as packet transmission which helps to identify the misbehaving nodes in wireless sensor network. Analytical and simulation experiment result shows that the proposed scheme detects the attackers in Wireless Sensor Network in efficiently and robustly with the cost of reasonable overheads.

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

I. Introduction

The adversaries may present the Wireless networks which can be deployed in hostile environments. Wireless networks are usually deployed in an unsupervised manner and it is controlled remotely by the network operator controlled it remotely [22]. Specifically, an attacker can spoof the 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. The common sensor network protocols fail to find the more aggressive attackers, including cluster formation, routing, and data aggregation, thereby causing continual disruption to the network operations [24]. Therefore, an adversary with compromised nodes can create confusion between the nodes in the wireless networks. So, the detecting and revoking of compromised nodes in the network is an important task.

Spoofing attacks can further create 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. Many spoofing attack possibility can be found in a broad survey [3], [4]. Moreover, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks in a large-scale network 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 to eliminate them.

Many approaches have been introduced so far 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. Attackers who have different locations than legitimate wireless nodes are concerned, spatial information is used not only to 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.

1.1 Overview of proposed model

Fig. 1 shows overview of the proposed model. The nodes are clustered and all the nodes are having the Watchdog mechanism for monitoring their neighboring nodes. If the Watchdog finds the attacker it passes the alarm message to the Cluster head (CH) which eliminates the attacker. The spatial correlation of Received Signal Strength (RSS) is used to detect the spoofing attacks. The K-Means clustering approach and Watchdog mechanism are implemented to detect the spoofing attack and to localize them in wireless sensor network.

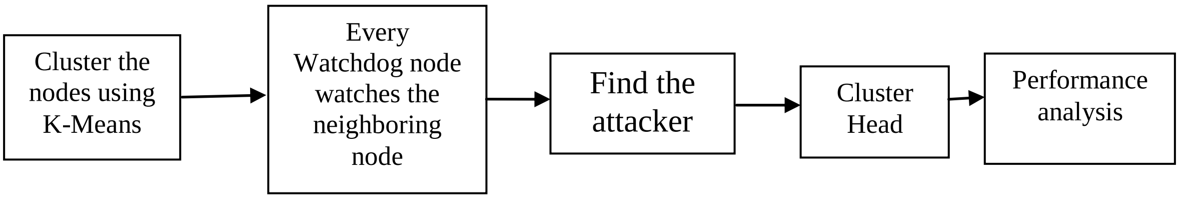
Cluster the nodes using K-Means
Every Watchdog node watches the neighboring node
Find the attacker
Cluster Head
Performance analysis

Figure 1. Block diagram of proposed system

The rest of this article is organized as follows: In Section II some related works are discussed. In Section III the Dynamic Source Routing Protocol is discussed. 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 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 to 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 where forge-resistant relationships is used 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’s 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 the attack is detected. None of the existing work can determine the number of attackers when there are multiple adversaries spoof with the same identity. Additionally, the proposed approach can accurately localize multiple adversaries even through the attackers vary in their transmission power levels to spoof the system of their true locations.

III. Dynamic Source Routing Protocol

DSR is a reactive routing protocol i.e. 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 addresses of the intermediate nodes of the route in the packets. DSR is beacon-less which means that 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 that each node is capable to save the best way to a destination. Also if any changes appear 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 the performances degrade. So AOMDV protocol is consider for this research work.

IV. Ad Hoc On Demand Multipath Distance Vector (AOMDV)

On-demand Multipath protocol called Ad hoc On-demand Multipath Distance Vector (AOMDV) is based on a prominent and well-studied on-demand single path protocol known as Ad hoc On-demand Distance Vector (AODV) [24, 25]. AOMDV is the extension of AODV protocol which is used to discover multiple paths between the source and the destination in every route discovery. Multiple computed paths are guaranteed for loop-free and disjoint paths.

AOMDV has three significant aspects compared to other on-demand multipath protocols. First, it does not have high inter-nodal coordination overheads like some other protocols (e.g., TORA, ROAM). Second, it ensures disjointness of alternate routes via distributed computation without the use of source routing. Third, AOMDV finds alternate paths with minimal additional overhead over AODV by exploiting the already available alternate path routing information as much as possible. AOMDV can be applied even in the presence of unidirectional links with additional techniques to help discover bidirectional paths in such scenarios.AOMDV shares several characteristics with AODV. AOMDV finds routes on demand using a route discovery procedure. In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. 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.

The mechanism used in AOMDV protocol to ensure the disjointness property are: at the beginning each node receives a RREQ packet and (a node can distinguish if it is the first time that examines a RREQ packet through the sequence number; it is the same mechanism used in AODV protocol) check itself whether it is neighbor (a one-hop distance) to the source or not. If it is, inserts its ID in a list called first-hop list. Intermediate nodes check current receiving a RREQ packet whether it has already received the same from the same neighbor of the source. It controls the first-hop list to verify it. If in the first-hop list there is no ID of the neighbor then it updates its first-hop list with the identifier found in the RREQ packet. An analogous mechanism is done in the Reply Phase where each node, near to the destination that receives a RREP, records its identifier in a list called last-hop list. Both lists (first-hop and last-hop lists), are used to make sure the disjointness property. Note that AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency [9].

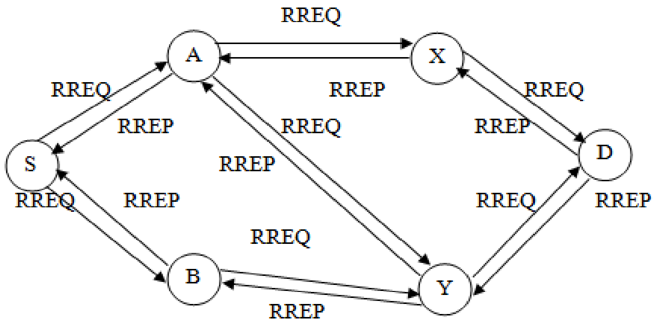

Figure 2: AOMDV protocol working

For example consider the situation in the 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 that 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 is 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. If it is active, it does not respect the property of link-disjointness. AOMDV can be used to find node-disjoint or link-disjoint routes. 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 to 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. The three mechanisms used in AOMDV protocol are Route Discovery, Route Reply and Route maintenance. It had two main components:

1. Route update rule to establish and maintain multiple loop free paths at each node.
2. A distributed protocol to find link disjoint paths.

V. K-Means Approach Using Received Signal Strength (RSS).

For spoofing detection, use the uniqueness of spatial information, instead of using the location information 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. Though it is affected by random noise, multipath effects, and environmental bias, RSS is measured at a set of landmarks reference points with known locations which is 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 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 existing K-Means clustering approach and the proposed Watchdog mechanism are discussed in the following section.

The RSS-based spatial correlation inherited from wireless nodes detects spoofing attack. The RSS readings from a wireless node may be fluctuated and clustered together. The RSS readings over time from the same physical location 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 reading is 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 the 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 centeroid.
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
          close to its own cluster, move it into the closest cluster.
Step 4: Repeat 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

5.1 Watchdog Mechanism.

The watchdog is a monitoring mechanism that helps to identify the misbehaving nodes in wireless sensor network. In this approach, each sensor node has its own watchdog that monitors and records its neighbors' behaviors in one hop such as packet transmission. Figure (3) illustrates how the watchdog works. The source node S wants to send the packets to its destination node D through their neighboring nodes A, B and C. The source node S sends a packet to its neighboring node A, the watchdog in S verifies whether A forwards the packet to B by using the sensor's overhearing ability within its transceiver range.

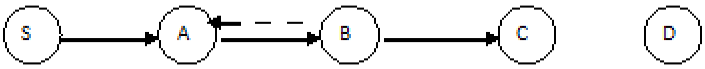

Figure 3: working of Watchdog Mechanism

In the same manner the neighboring node A sends the packets to its neighboring node B, the watchdog in A verifies whether B forwards the packet to node C. In this mechanism, A stores all recently sent packets in its buffer, and compares each packet with the overheard packet to see whether there is a match. If yes, the packet is forwarded by B and A will remove the packet from the buffer. If a packet remains in the buffer for a period longer than a pre-determined time, the watchdog considers B when it fails to forward the packet and will increase its failure count for B. If a neighbor's failure count exceeds a certain threshold, it will be considered as a misbehaving node by A. Watchdog works similar to trust mechanism where the trust model evaluates each sensor's trustworthiness based on the past behaviors. The watchdog mechanism can detect misbehaving nodes at forwarding level and not just the link level. The watchdog mechanism for attack detection in wireless sensor network is given in the Figure 4.

```
Watchdog Mechanism for detecting and localizing the attackers in WSN:
Input    : T =A topology in which m number of malicious node present in a set of n number of
             sensor  nodes.
Output :  O = Set of clusters which are having watchdog nodes used to find malicious nodes Set
              initial parameter of network

Step 1: Mobile Sensor Node's = N;
        MAC layer = 802.11
        Routing = AOMDV
        Attacker nodes = False Misbehavior
       //Attacker launches false misbehavior
       Attacker-node (capture vulnerable node information && send =false alarm packet)
       If (Sink detects a discontinuous sequential number)
         {      Infected;
        Broadcasts an alert packet;
           }
Step 2 : For (Intermediate node check for the missing sequence in its cache)
         { If
         {    Missing packet found;
         Send back to the node;
              }
         Else {
          Sends back a normal response packet;
             }}
Step 3 :If (Sink receive number of response packets)
        {     Intermediate node does not send any response, its identity recorded;
          }
Step 4 : Generate trace file for further analysis
Step 5 : Do (analysis trace for detection)
         {     Analyze the nodes of the routing path, Mark the malicious node;
         Find infection ratio;
        Mark the suspicious node and Block the Malicious Node;
          }
```

Figure 4: Watchdog mechanism for attack detection in WSN

VI. Experimental Analysis

Simulations are conducted to analyze the performance of proposed Watchdog mechanism 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. 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.

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

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 is high when increasing the packet delivery ratio and decreasing the packet drop. 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 comparison

Time (ms)	Throughput	
	K-Means	Watchdog mechanism
12	9	20
15	15	28
18	26	37
21	52	64
24	75	80

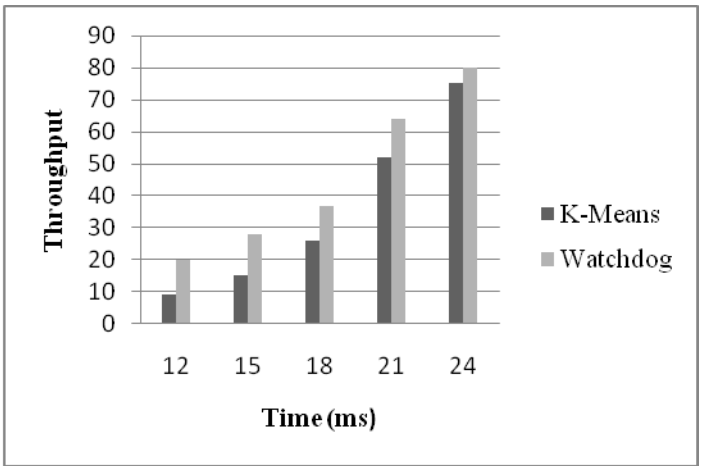

Figure 5: Throughput comparison between K-Means and Watchdog mechanism

From the simulation results, it is noted that the high throughput is achieved by Watchdog mechanism. The throughput achieved by the methods K-Mean and Watchdog mechanism for various time slots are provided in table 2 and the same is flashed in fig 5. The watchdog mechanism achieves high throughput than the K-Means approach for all time intervals. The K-Means approach achieves the throughput of 75% in the time duration of 24 milliseconds where as the watchdog mechanism achieves 80% throughput in the same time duration. It is noted that the watchdog yields 5% higher than the K-Means approach.

The PDR ratio is measured in the percentage as

$$\text{PDR} = \left(\frac{P_r}{P_s}\right) \times 100$$

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	WDM
12	15	25
15	32	42
18	54	65
21	68	79
24	82	93

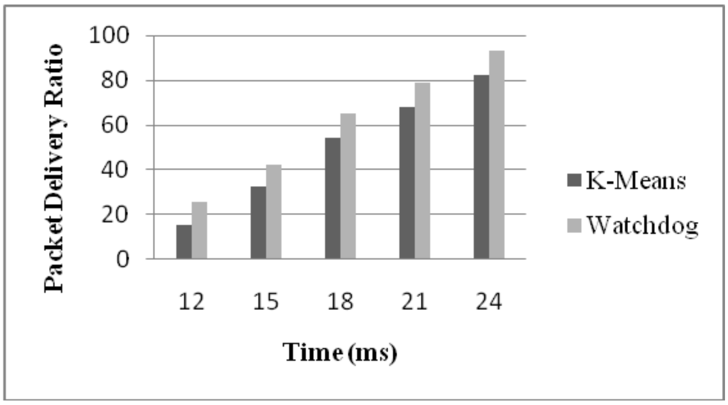

Figure 6: PDR comparison between K-Means and Watchdog mechanism

Packet Delivery Ratio is the ratio between sum of total number of packets received by destination and the 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 Watchdog approach. The results in table 3 show the Packet Delivery Ratio of Watchdog mechanism 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 Watchdog mechanism, the watchdog yields highest Packet Delivery Ratio. From this study, it is found that the reliability of Watchdog algorithm is better than K-Mean approach and it is noted that Watchdog approach is efficient than the other approach.

Packet Drop Rate is the difference between number of sent packets and received packets by the source and destination respectively. It is used to know the percentages of packets lost 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)

Table 4: Packet Drop Rate

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

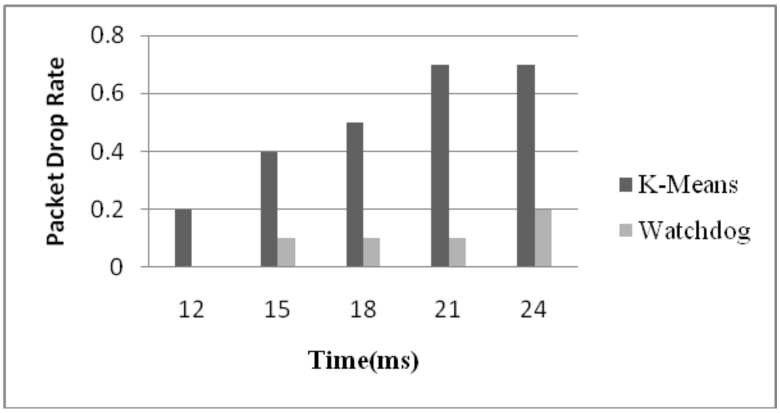

Figure 7: Packet Drop comparison between K-Means and Watchdog mechanism

From the simulation results, it is noted that less packet drop is achieved by Watchdog mechanism. The percentage of the Packet Drop Rate is defined as number of packets dropped divided by the total number of packets send. The Packet Drop Rate of the methods K-Mean and Watchdog mechanism for various time slots are provided in table 4 and the same is flashed in fig 7. The Packet Drop Rate achieved by K-Means is 0.4% in the time duration of 15 milliseconds where as the watchdog mechanism decreases the Packet Drop Rate from 0.4% to 0.1% in the same time duration. It is noted that the watchdog mechanism achieves more than 0.3% better result than the K-Means approach.

VII. Conclusion

In this paper, the Watchdog mechanism 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 Watchdog mechanism are analyzed in 802.11 networks in Wireless Sensor Network. Results revealed that the proposed Watchdog mechanism is better for detecting and localizing the misbehaved nodes. The experimental result also proved that the proposed mechanism achieves higher accuracy than K-Means methods. Therefore proposed scheme can quickly detects the spoofing attackers. Further, the scheme may propose to various types of attack detection model to find the attacker and localize the same to extend the battery life and achieve the high results in Wireless Sensor Network.

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]. 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.

[25]. 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.