Australian Journal of Basic and Applied Sciences, 9(5) March 2015, Pages: 229-237

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Development of OLSR based Selective Jamming Attack Detection Mechanism in Wireless Sensor Networks

[1]F. Vincylloyd, [2]Dr. B. Anand, [3]Mr.J. Jijin Godwin

[1]*RVS Technical Campus – Coimbatore, Faculty of Engineering, ECE Department, Anna University, Coimbatore, India.*
[2]*Hindusthan College Of Engineering and Technology, EEE Department, Anna University, Coimbatore, India.*
[3]*Velammal Institute of Technology, ECE Department, Anna University, Chennai, India.*

ARTICLE INFO

Article history:
Received 12 November 2014
Received in revised form 26 December 2014
Accepted 29 January 2015
Available online 10 February 2015

Keywords:
Wireless Sensor Networks, MAC protocol, Optimized Link State Routing protocol, Selective Jamming Attacks.

ABSTRACT

Background: Wireless Networks are made upon a shared medium that makes it simple for adversaries to establish a jamming attacks. The jamming attacks can rigorously interact with the normal operation of wireless networks. Objective: It be easily accomplished by an attacker releasing radio frequency signals that do not follow an underlying MAC protocol. Hence, a security mechanisms are needed to cope up with the jamming attacks. In this paper, the problem occurred in wireless sensor networks due to selective jamming attacks are addressed. Results: Hence, based on protocol semantics, a security mechanisms are proposed in this paper. Optimized Link State Routing protocol is incorporated to maintain a stable route between the source and destination. Error Tolerant Model (ETM) is used to check the network contains the jammer or not. Malicious node detection algorithm is implemented to identify the malicious nodes based on its behavior. It is monitored based on the Virtual Watchdog Timer strategy. Conclusion: The experimental results shows that the proposed method detects the selective jammer better than the existing selective jamming attack detection. Also, the energy consumption, packet drop are also reduced than the existing method.

To Cite This Article: F. Vincylloyd , Dr. B. Anand, Mr.J. Jijin Godwin., Development of OLSR based Selective Jamming Attack Detection Mechanism in Wireless Sensor Networks. ***Aust. J. Basic & Appl. Sci.,*** *9(5): 229-237, 2015*

INTRODUCTION

Wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. A major issue in WSN is network security, they are susceptible to the kind of radio interference attacks due to their distributed nature. These attacks are called as jamming attacks, it can be simply established by any node. An adversary node can compromise a sensor node and modifies the integrity of the data, inject fake messages, eavesdrop on messages and damage the network resources. In particularly, Jamming attack can cause damages about the performance and robustness of the network. Thus one of the challenges in formulating trusted WSNs is to facilitate high security features. Any wireless device with a transceiver can able to eavesdrop the ongoing transmission. The malicious node corrupts the transmitted packet by causing electromagnetic interrupt in the network functioning frequencies and the targeted receivers (Simon, M.K., 1994). Jamming consequences an increased energy consumption, loss of link reliability, disruption of end to end routes and extended packet delays. Jamming may be malicious with the purpose to avoid communication of an adversary node or it may be non-malicious with the purpose of unintended channel interference.

The jammer transmits active signals over the channels that interrupt with the signal broadcast by the server, which is shown in fig.1. In selective jamming attacks, the adversary node selectively targets particular packets by exploring the details of network protocols at various layers present in the protocol stack. To establish these attacks, the adversary node should be able to implement a classify-then-jam policy before the completion of a wireless transmission. These policy can be represented by classifying transmitted packets using protocol semantics (Thuente, D. and M. Acharya, 2006; Brown, T.X., 2006) or based on the decoding the packets on the fly (Wilhelm, M., 2011). The selective jamming needs an intimate details of the physical layer and also the specifics of the upper layers.

Corresponding Author: F. Vincylloyd, RVS Technical Campus – Coimbatore, Faculty of Engineering, ECE Department, Anna University, Coimbatore, India..

In this paper, a novel security mechanism is proposed for the detection of selective jamming attacks using protocol semantics. The effectiveness of jamming in WSN using OLSR protocol and introduces an Error Tolerant Model to facilitate the jammer detection of such networks. The OLSR protocol is used to discover and establish stable routing paths. The nodes behavior is periodically monitored based on virtual watchdog timer. The proposed method results better detection of selective jamming attack than the existing method.

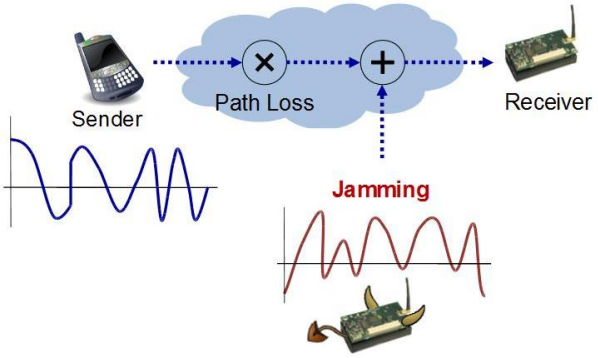

Fig. 1: Jamming attacks.

The remainder of this paper is organized as follows. Section 2 summarizes the related works about jamming attacks in WSN. Section 3 describes about the proposed system. Section 4 describes the performance analysis. And finally, the paper is ended with the conclusion and future work at section 5.

Methods:

The aim of the jammer is to interrupt the normal operation of the broadcast system that results in higher waiting time and higher energy consumption. *Proano et al* designed a packet hiding methods for preventing selective jamming attacks. The selective jamming attacks were established by executing the real time packet classification on physical layer. This scheme integrates three methods to protect the real time packet classification by integrating the cryptographic primitives with the physical layer characteristics (Proano, A. and L. Lazos, 2012). *Cakiroglu et al* proposed a query based jamming detection algorithm. This algorithm was designed to prevent the jamming attacks. This algorithm uses an anomaly based method and it performs in a distributed manner. This algorithm was validated based on three criteria like detection rates, false positive rates and communication overheads (Cakiroglu, M. and A.T. Ozcerit, 2011). *Chen et al* formulated a framework for energy efficient adaptive jamming of adversarial communications. The jammer enhances its strategy as energy efficient by obtaining the targeted throughput result. A frequency hopping voice network was observed to regulate the optimal plan policy for proactive frequency jammer. CSMA packet protocol was examined on behalf of changing packet arrival rates at the nodes. The feedback control loop employs observable feedback to infer the network parameters. *Cheng et al* 2013 formulated an algorithm for mobile jammer localization in wireless sensor networks. This algorithm comprising the jammer and predicting the next jammer location. The algorithm was based on the received signal strength of jamming signals known as RSS based mobile jammer traction (Cheng, T. and P. Li, 2012).

Jeung et al introduced an adaptive rapid channel hopping technique. This scheme uses deception mechanism and dwell window to prevent the smart jammer attacks. The dwell window regulate the transmission time based on jammers capability. The another deception mechanism forces the jammer to attack an sedentary channel based on deceiving the jammer. *Ju et al* (2012) proposed a jamming attack detection and rate adaption technique for IEEE 802.11 multi hop tactical networks. The rate adaption method notices the jamming attack and chooses the data transmission mode. *Kim et al* (2012) proposed a localization approach to locate the wireless nodes. The power adaptation methods was used to discover the location of the jammer. Those properties were used to generalize the locations of jammed nodes. *Lee et al* (2011) developed a timely and robust key establishment model against jamming attack under critical wireless networks. A frequency quorum rendezvous scheme was utilized to prevent jamming during the key establishment stage. *Lee et al* (2010) designed a randomized channel hopping strategy for anti-jamming communication. Quorum Rendezvous Channel Hopping (QRCH) system was proposed to avoid jamming attacks. The quorum system was used to guarantee that the node exchanges the pending messages within a bounded time. It permits the nodes can simultaneously transmit the messages to multiple receivers.

Moumena et al (2014) proposed a fast anomaly detection using boxplot rule for multivariate data in presence of jammer. A centralized cooperative compressive spectrum sensing method was constructed based on the integration of graphical

boxplot rule and compressive sampling approach. The conventional signal and white Gaussian noise was converted into a digital signal based on analog to information converter through random demodulator. Cooperation between cognitive radios permits the users to identify the anomalies in the presence of jamming attack signal. *Sasikala et al* (2013) proposed a modified ant system to detect the jamming attack in WSN. The mechanism includes payment for pushback, strong authentication, network resources and identification traffic. *Sun et al* (2011) introduced a jammer localization method. The victim nodes share the location details at the border with their neighbor nodes. It calculates the convex hull for the group of target nodes and mines the resultant minimum covering circle. *Zhenhua et al* (2012) introduced a mechanism to localize a jammer based on the neighbor node changes. The jammer location was calculated based on solving a least squares problem, which exploits the changes of communication area. *Liu et al* (2012) proposed a randomized distributed scheme. It permits nodes to launch and regulate the control channel in presence of jammer. The algorithm was used for unique identification for the group of compromised nodes.

Chiang et al (2011) formulated a cross layer jamming detection and mitigation in wireless broadcast networks. A code tree system was used to deliver input to the physical layer. Each receiver conjoins with the transmitter to identify any jamming which interrupts the receivers. Each benign user was guaranteed in order to eliminate the attacker after some limited number of losses based on arbitrarily high probability. *Jiang et al* (2011) introduced a framework for providing survivability against jamming attack for multi radio multi-channel wireless mesh networks. Here, efficient routing and channel assignment techniques were used to relieve the interruption occurred by normal nodes and jamming nodes. The greedy scheduling algorithm was used with dynamic channel assignment to schedule the network and jamming traffic. A greedy static edge channel assignment algorithm was used to assign a channel to an edge at the beginning and maintained all over the time slots. The global restoration and local restoration strategies were considered to support a tradeoff between network throughput after restoration and latency.

Wang et al (2013) proposed a collaborative jamming and collaborative defense in cognitive radio networks. The dissemination of jamming signal was computed based on the random deployment of jammers. The jamming and defending methodologies were incorporated by the jammers and genuine users. The channel availability was analyzed when the genuine users randomly select the channels and jammers. A multi-tier based cooperative defense mechanism was utilized to explore the temporal and spatial diversity for the genuine users. *Lasc et al* (2011) developed an authentication and key agreement protocol against jamming attacks for mobile satellite communications. *Mpitziopoulos et al* (2009) proposed a Jamming.

Avoidance Itinerary Design (JAID) algorithm. It computes the optimal routes for mobile agents. Also computes the itineraries to bypass the jammed regions. The algorithm only modifies the pre-jamming area to improve the promptness, if the jammed nodes are small. Otherwise, the algorithm reconstructs the agent excluding the jammed areas.

Niu et al (2012) designed an anti-chirp jamming communication method based on cognitive cycle. The chirp jamming sensing module was developed to detect and identify the parameters of chirp jamming based on periodogram and kalman filter. The chirp jamming decision making component makes decision on transmission power and communication frequency. They were computed based on simple arithmetic computation. *Ho et al* (2012) discussed about the distributed detection of mobile malicious node attacks in WSN. A sequential hypothesis testing was applied to discover the nodes that are malicious. *Sung et al* introduced a neighbor based malicious node detection scheme for WSN. Each node includes the confidence and its neighbors confidence indicating the track records in reporting previous events appropriately. *Ould et al* (2012) presented a distributed fault tolerance for error detection across heterogeneous WSN. *Warriach et al* (2012) proposed a hybrid fault detection approach in WSN. *Banerjee et al* (2014) introduced a fault detection and replacement scheme.

1.1 Olsr based jamming attack detection mechanism:

This section describes about the proposed detection mechanism against selective jamming attacks. Fig.2. illustrates the flow of the proposed method for the detection of the selective jamming attacks.

The OLSR protocol is used to discover and maintain the stable link routing paths. After the routes are discovered, Error Tolerant Model (ETM) is applied to find the network includes any jammer node or not. If any jammer is present, then the route discovery procedure gets repeated until the path doesn't contain any jammer node. Also, check for the malicious nodes based on the node behavior with the help of virtual watchdog timer. If any malicious node is detected, then the location of the node is estimated to block the malicious node for secure data transfer.

1.2 OLSR Protocol:

OLSR uses hello and topology control packets to establish and broadcast link state information throughout the sensor network. Hello packets are used for discovering the details about the link status message and host. TC messages are used for distributing information about advertising neighbors, it includes atleast multipoint relay selector list. An

individual node can use this topology details to estimate the next hop destination for all nodes based on shortest hop forwarding paths. At each node determines 2 hop neighbor details based on hello message and makes a distributed election of a group of multipoint relays (MPR). The routing paths for TC packets is not mutual among all nodes but changes depend on the source.

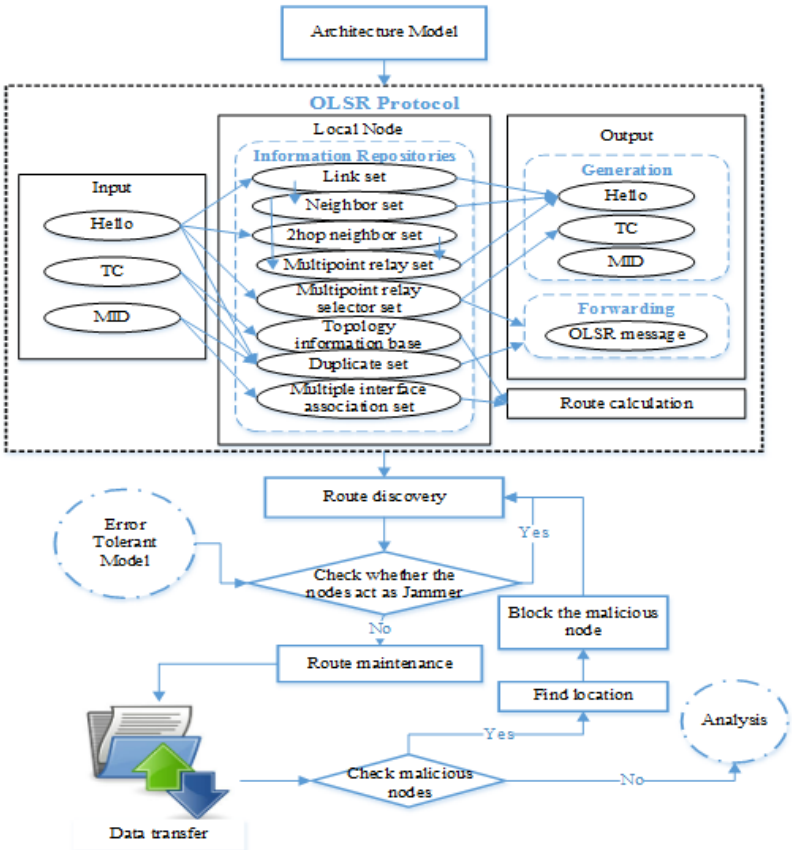

Fig. 2: Structure of the proposed detection mechanism.

Multiple Interface Declaration (MID) messages can be used to inform the other host that announcing the host has many OLSR interface addresses. The main advantage of this protocol is, it does not need any central administrative scheme. Also, the flooding is minimized by MPRs. The suitable working environment for OLSR protocol is a condensed network. Here the communication is focused among a hug e number of nodes. It reduces the control overhead pushing the MPR to disseminate the updates of the link state. It immediately knows the eminence of the link and it extends the quality of service.

1.3 Error Tolerance Model:

To tackle errors in WSN, the proposed model follows the following two steps:

1. Error detection: During the data transmission, if the specific functionality is faulty and spot it down to predict the function properly in the future transmission.
2. Error recovery: It deals with the system to recover from the faulty conditions.

Usually, there are two types of error detection techniques: one is self-diagnosis and the other one is cooperative diagnosis. Some of the errors can be detected by the sensor node itself. For instance, errors occurred due to the exhaustion of battery can be identified by the node itself. The residual energy of the battery can be calculated based on measuring the current battery voltage.

1.4 Generation of Hopping Sequence:

In order to defend the privacy of the control channel, the hopping sequence need to fulfill the following properties:

1. Independence; details of one sequence do not expose any details regarding another,
2. Knowledge of previous hops does not expose any details about the future ones;
3. High minimum hamming distance; during interpreted as code words. The sequence must have high hamming distance, hence the compromised node can be exclusively recognized.

1.5 Misbehavior detection:

Suppose that the network can potentially detect a particular type of misbehavior. It is likely that any such misbehavior detector has some false positives. As a result, it might not take action until it observes several repeated offenses by the same node. Watch dog device that detects faults and initiates corrective actions. Here, Watchdog virtual timer is used to monitor the nodes behavior. If any unauthorized or irrelevant behavior is sensed from the sensor nodes, then the location of the node is identified and blocked.

1.5.1 Identification of compromised nodes:

The compromised nodes are identified based on their assigned hopping sequences. When the control channel is denied, nodes start hopping based on their pre-assigned hopping order. If suppose the jammer negotiates one of the nodes d_j, it can find the consistent hopping sequence a_j. The unique order a_j discloses the uniqueness of the compromised node d_j.

Algorithm 1:

1. Initialize
2. $d(a_j, a_{jam}) = 0, \forall j$
3. $j=1; i=0; N \leftarrow \phi$
4. **while** J is false do
5. **for** $m=1, m \leq M, m++$ do
6. **if** $a_j(i)$ not jammed then
7. $d(a_j, a_{jam}) = d(a_j, a_{jam})+1$
8. **end if**
9. **if** $d(a_j, a_{jam}) < \frac{B-1}{B}m - \delta_m$ && $m > h$ then
10. J=true
11. $N \rightarrow d$
12. Break
13. **else**
14. i++
15. **end if**
16. **end for**
17. **if** J is true then
18. break
19. **else**
20. j++
21. **end if**
22. **end while**
23. return N

If the calculated hamming distance is below the estimated hamming distance, by a margin of δ_m, then the compromised node has been effectively detected. δ_m is calculated based on the variance of the hamming distance, that is given by $\frac{B-1}{B}m$. Here m is the number of slots observed. This process gets repeated in a round robin fashion. The estimated hamming distance H [d (a_j, a_l)] among two random sequences a_j and a_l as a function of their length M is

$$E\left[d\left(a_j, a_l\right)\right] = \frac{B-1}{B}M \quad (1)$$

Based upon the above equation, the compromised nodes are successfully identified and removed from the data transmission.

1.2 Performance analysis:

In this section, the performance of the proposed OLSR based jamming attack prevention mechanism is presented and compared with the Preventing Selective Jamming Attack (PSJA) method without the OLSR protocol. The performance is validated based on the following metrics: packet drop, energy consumption, number of active nodes and packet received ratio.

1.2.1 Packet Loss Ratio:

Packet loss is the failure of one or more transmitted packets to arrive at their destination. The proposed OLSR-SJAD results lesser packet drop than the Preventing Selective Jamming Attack (PSJA) method without the OLSR protocol. It improves the packet delivery ratio and it yields the reliable system performance. It is achieved with the help of OLSR protocol in case of the link failure. The following formula is used to calculate the packet loss.

$$Packet\ Loss = number\ of\ packet\ sent - number\ of\ packet\ received \quad (2)$$

If any node is detected as a malicious or jammer node, then the OLSR protocol can find another

trusted route to forward the data. Fig.3. shows the comparison of packet loss between the proposed OLSR-SJAD and the PSJA method.

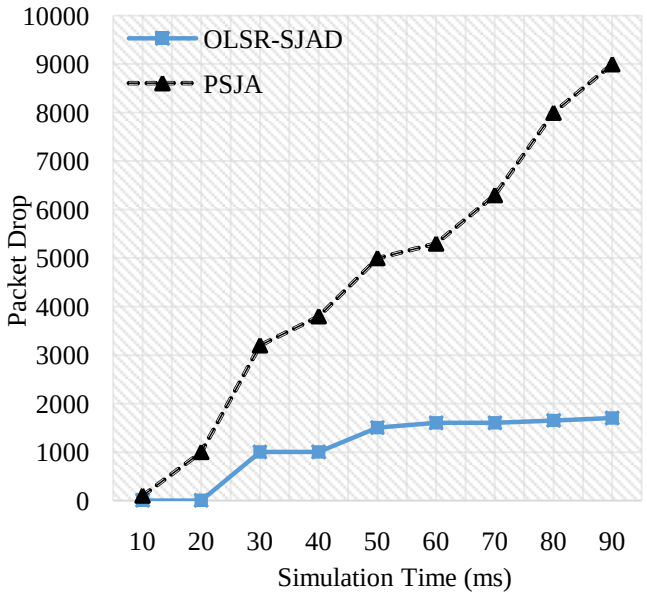

Fig. 3: Analysis of packet drop between the proposed OLSR-JAD and existing PSJA method.

1.3. Energy Consumption Analysis:

The energy consumption by the network over a period of time is based on the following categories:

- Energy spent for sensing the channel,
- Energy spent throughout the transmission range,
- Energy spent during the reception phase and
- Energy spent for error detection and recovery.

Based upon the above categories, the overall energy consumption can be computed. Fig.4. shows the proposed OLSR-SJAD mechanism utilizes lesser energy usage than the existing PSJA method.

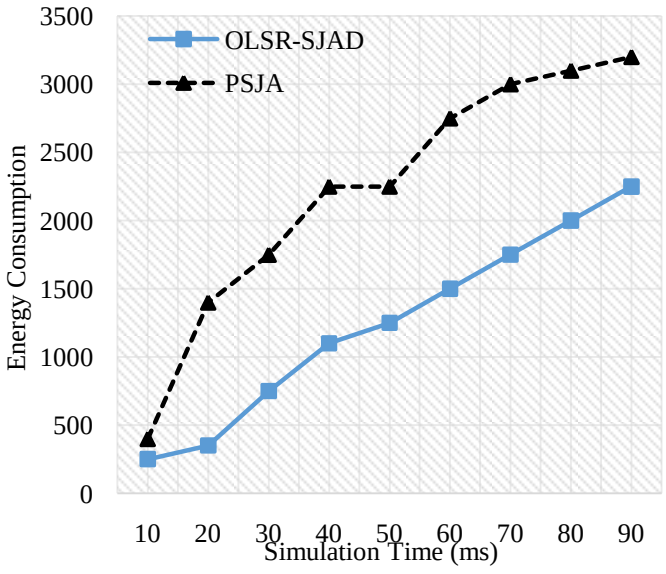

Fig. 4: Analysis of energy consumption for data transfer between OLSR-JAD and PSJA method.

1.4. Packet Received Observation:

The active nodes must be selected cautiously so that the sensor nodes can work long adequate and reliable to forward the data from source to corresponding destination. The active nodes are selected based on their connectivity between their neighbor nodes and their residual energy. If a system is frequently reducing the active nodes, then it results high level of packet loss. But the proposed system maintains more number of active nodes throughout

the data transfer which is obviously shown in fig.5. Hence the proposed OLSR-SJAD yields better and scalable results than the existing methods.

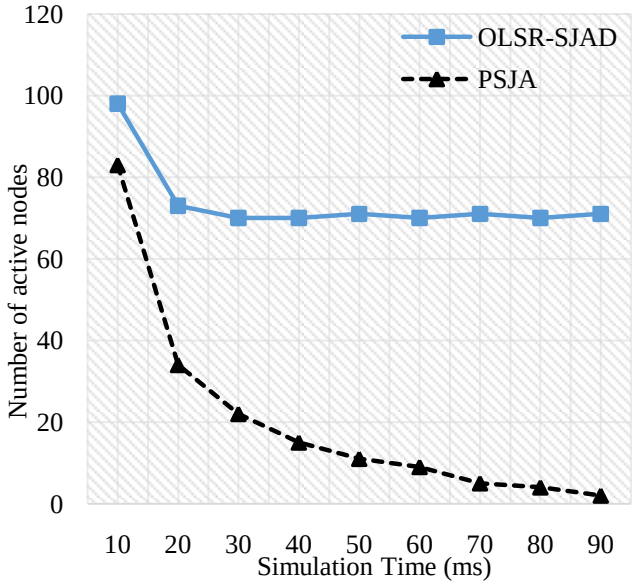

Fig. 5: Analysis of active node calculation between OLSR-JAD and PSJA method.

The packet received ratio is the ratio of the number of delivered data packet to the destination. It explains the level of received data to the destination.

$$Packet\ received = \frac{\sum number\ \ of\ packet\ \ received}{\sum Number\ \ of\ packet\ \ sent} \quad (3)$$

The above equation is used to compute the packet received ratio. Fig.6. depicts the packet received rate analysis for the proposed and the existing method. It confirmed that the OLSR-SJAD yields higher packet received rate than the existing PSJA method.

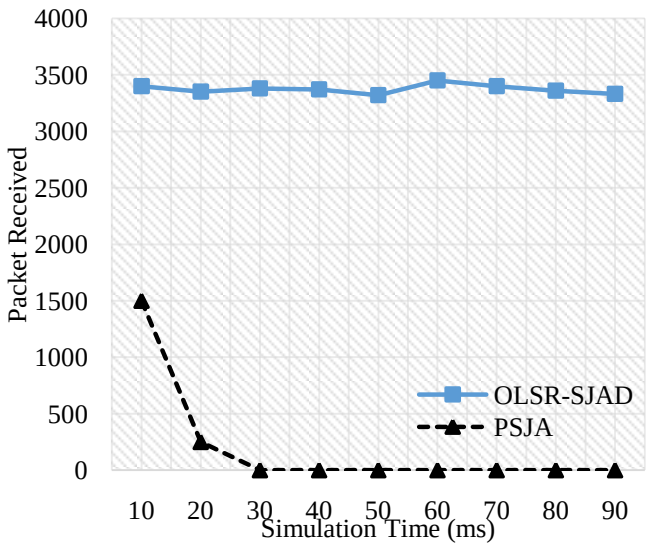

Fig.6: Analysis of number of packets received between OLSR-JAD and PSJA method.

Table 1: Analysis of OLSR-JAD Performance

Evaluation metrics	Values
Packet delivery ratio	11.82
Average end to end delay	1.42
Average number of hops	2.4
Control packet overhead	21711
Throughput	5944.8
Data packets sent	12101
Data packets received	1431

Simulation end time	55.36
Total delivery time	2037.61
Total number of hops	3431
Dropped reply messages	0
Maximum number of hops	3
Minimum number of hops	2

RESULTS AND DISCUSSION

This paper addresses the problem of selective jamming over wireless sensor networks. The proposed model OLSR-SJAD mechanism uses the OLSR protocol for better link stability and route maintenance. An Error Tolerant Model is incorporated to efficiently identify the jammer device that selectively target the source and destination nodes. Also, the malicious nodes is identified based on the watch dog timer and the proposed algorithm. The experimental results guaranteed that the proposed model can identify the selective jamming attack and block the malicious nodes from the data transfer. The proposed method results better packet delivery ratio with reduced energy consumption and packet delay than the existing PSJA method.

In future, the proposed method is incorporated with an energy efficient and secure routing protocol to provide high level security.

REFERENCES

Banerjee, I., A. Datta, S. Pal, S. Chatterjee and T. Samanta, 2014. "A Novel Fault Detection and Replacement Scheme in WSN," in *Recent Advances in Intelligent Informatics*, ed: Springer, pp: 303-310.

Brown, T.X., J.E. James and A. Sethi, 2006. "Jamming and sensing of encrypted wireless ad hoc networks," in *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing*, pp: 120-130.

Cakiroglu, M. and A.T. Ozcerit, 2011. "Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks," *Turkish Journal of Electrical Engineering & Computer Sciences*, 19: 1-19.

Chen, J., S. Sen, M. Chiang and D.J. Dorsey, 2013. "A framework for energy-efficient adaptive jamming of adversarial communications," in *Information Sciences and Systems (CISS), 2013 47th Annual Conference on*, pp: 1-6.

Cheng, T. and P. Li, 2012. "An Algorithm for Mobile Jammer Localization in Wireless Sensor Networks," in *Proceedings of the 2012 Second International Conference on Electric Information and Control Engineering*- 3: 90-94.

Chiang, J.T. and H. Yih-Chun, 2011. "Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks," *Networking, IEEE/ACM Transactions on*, 19: 286-298.

Ho, J.W., M. Wright and S.K. Das, 2012. "Distributed detection of mobile malicious node attacks in wireless sensor networks," *Ad Hoc Networks*, 10: 512-523.

Jeung, J., S. Jeong and J. Lim, 2011. "Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN," in *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011*, pp: 1231-1236.

Jiang, S. and Y. Xue, 2011. "Providing survivability against jamming attack for multi-radio multi-channel wireless mesh networks," *Journal of Network and Computer Applications*, 34: 443-454.

Ju, K. and K. Chung, 2012. "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks," *International Journal of Security & Its Applications*, 6.

Kim, Y.S., F. Mokaya, E. Chen and P. Tague, 2012. "All your jammers belong to us—Localization of wireless sensors under jamming attack," in *Communications (ICC), 2012 IEEE International Conference on*, pp: 949-954.

Lasc, I., R. Dojen and T. Coffey, 2011. "Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications," *Computers & Electrical Engineering*, 37: 160-168.

Lee, E.K., S.Y. Oh and M. Gerla, 2010. "Randomized channel hopping scheme for anti-jamming communication," in *Wireless Days (WD), 2010 IFIP*, pp: 1-5.

Lee, E.K., S.Y. Oh and M. Gerla, 2011. "Timely and robust key establishment under jamming attack in critical wireless networks," in *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011*, pp: 1237-1242.

Liu, S., L. Lazos and M. Krunz, 2012. "Thwarting Control-Channel Jamming Attacks from Inside Jammers," *Mobile Computing, IEEE Transactions on*, 11: 1545-1558.

Moumena, A. and A. Guessoum, 2014. "Fast anomaly detection using Boxplot rule for multivariate data in cooperative wideband cognitive radio in the presence of jammer," *Security and Communication Networks.*

Mpitziopoulos, A., D. Gavalas, C. Konstantopoulos and G. Pantziou, 2009. "JAID: An algorithm for data fusion and jamming avoidance on distributed sensor networks," *Pervasive and Mobile Computing*, 5: 135-147.

Niu, Y., F. Yao, M. Wang and J. Chen, 2012. "Anti-chirp-jamming communication based on the cognitive cycle," *AEU - International Journal of Electronics and Communications*, 66: 547-560.

Ould-Ahmed-Vall, E., B.H. Ferri and G.F. Riley, 2012. "Distributed fault-tolerance for event detection

using heterogeneous wireless sensor networks," *Mobile Computing, IEEE Transactions on*, 11.

Proano, A. and L. Lazos, 2012. "Packet-hiding methods for preventing selective jamming attacks," *Dependable and Secure Computing, IEEE Transactions on*, 9: 101-114.

Sasikala, E. and N. Rengarajan, 2013. "A Novel Mechanism to Detect Jamming Attack in Wireless Sensor Network Using Modified Ant System," *International Review on Computers & Software*, 8.

Simon, M.K., J.K. Omura, R.A. Scholtz and B.K. Levitt, 1994. *Spread spectrum communications handbook* vol. 2: McGraw-Hill New York.

Sun, Y., R. Molva, M. Onen, X. Wang and X. Zhou, 2011. "Catch the Jammer in Wireless Sensor Network," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium*, pp: 1156-1160.

Thuente, D. and M. Acharya, 2006. "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," in *Proc. of IEEE MILCOM*.

Wang, W., S. Bhattacharjee, M. Chatterjee and K. Kwiat, 2013. "Collaborative jamming and collaborative defense in cognitive radio networks," *Pervasive and Mobile Computing*, 9: 572-587.

Warriach, E.U., K. Tei, T.A. Nguyen and M. Aiello, 2012. "Fault detection in wireless sensor networks: a hybrid approach," in *Proceedings of the 11th international conference on Information Processing in Sensor Networks*, pp: 87-88.

Wilhelm, M., I. Martinovic, J.B. Schmitt and V. Lenders, 2011. "Short paper: reactive jamming in wireless networks: how realistic is the threat?," in *Proceedings of the fourth ACM conference on Wireless network security*, pp: 47-52.

Yim, S.J. and Y.H. Choi, 2012. "Neighbor-Based Malicious Node Detection in Wireless Sensor Networks," *Wireless Sensor Network*, 4.

Zhenhua, L., L. Hongbo, X. Wenyuan and C. Yingying, 2012. "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization," *Parallel and Distributed Systems, IEEE Transactions on*, 23: 547-555.