IOT: Jamming Attack Modelling And Evaluation

Ayushman Chhapariya[1], Neetu Sikarwar[2]
[2] Professor
[1, 2] Institute of Engineering Jiwaji University, Gwalior

Abstract- *The jamming attack that take place at physical layer and its classification in detail. It also provides modelling of jamming attack using activity- and sequential- modelling approach and evaluates the different jamming attack in variety of network situations. The paper proposes new possibility of the jamming attack i.e. intelligent cluster-based jamming attack and evaluates the performance impact of cluster-based jamming attack. Lastly, the paper discusses the requirements to design efficient defence mechanism against jamming attack.*

Keywords- Wireless sensor networks (WSNs), activity modelling, security attacks, jamming attacks, media access control (MAC).

I. INTRODUCTION

The research in WSN is growing in large perspective to offer the wide variety of application domains. The WSN consist of the large number of nodes, which sends the sensed information to the central base station (BS) [1]. The WSN node suffers from large energy constraint because of its limited battery power. The major requirement to achieve quality of service (QoS) in WSN is to reduce energy consumption with minimum delay and maximum throughput. These performance requirements are largely affected by security attacks, which happen at various layers of WSN. WSN is vastly invaded by the different kinds of jamming attacks at each layer. The paper mainly concentrates on jamming attacks, which occur at physical and medium access control (MAC) layer. Here, it is more effective and destructive because these layers are mainly responsible for allocating the resources. The different kind of active and reactive jamming attack effects on WSN constraints based behaviour, by increasing the energy consumption with increased delay and decreased throughput. These are very important performance parameter for deciding QoS of WSN. The different kinds of jamming attacks are constant jamming, deceptive jamming, random jamming, and reactive jamming. All these jamming attacks are modelled to understand the basic sequence of activities during their occurrences in the network. The author uses unified modelling language (UML) [5] based activity and sequential modelling approaches for modelling the behaviour of various jamming attacks. Activity modelling models the behaviour by considering different states and shows the various conditions, message transmission between the states. It is one of the useful ways to understand the intelligent behaviour of jamming attack. The activity modelling also gives the understanding of required security solution for reducing the effect of attack on WSN performance. Sequential modelling is one of the widely used ways to model the system using UML. It is used to illustrate the interactions between different entities of system.

II. MODELLING AND EVALUATION OF JAMMING ATTACK

This section models the behaviour of different types of jamming attack using sequential and activity modelling approaches under unified modelling language (UML). The differences between activity modelling and sequential modelling are, (i) activity modelling gives high-level understandings of the system functionalities while sequential modelling gives low-level dynamic interaction between the objects, (ii) activity modelling describes the data flow between users and system while sequential modelling illustrates the objects involved and messages exchanged during the data transfer. Here, the modelling of jamming attack using activity- and sequential- modelling gives the complete understanding of attack behaviour with its high level data flows, objects involved, and messages exchanged during the interaction of different objects.

2.1 Activity Modelling of Jamming Attacks

The activity modelling explains the functional view of a system by describing or representing logical processes, or functions. Here, each logical process is represented as a sequence of tasks and the decisions that govern when and how they are performed. Activity modelling is one of the UML representations for giving functional view of any processes or tasks [5, 8]. UML is designed to support the description of behaviours that depends upon the results of internal processes. The flow in an activity diagram is driven by the completion of an action. The activity diagram is useful tool to understand the basic flow of security attacks.

2.1.1 Constant Jamming

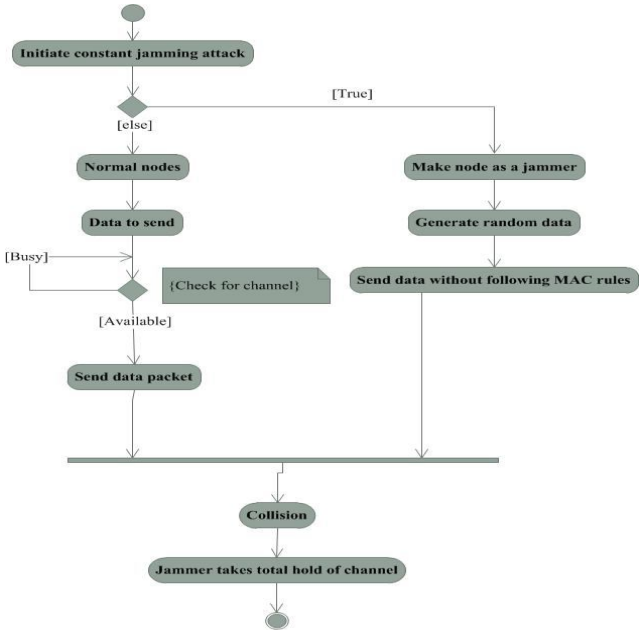

Figure 1: Activity modelling of constant jamming attack

Figure 1 shows the activity modelling of constant jamming attack. It gives insight of different activities that takes place during the execution of attack on a network.

2.1.2 Deceptive Jamming

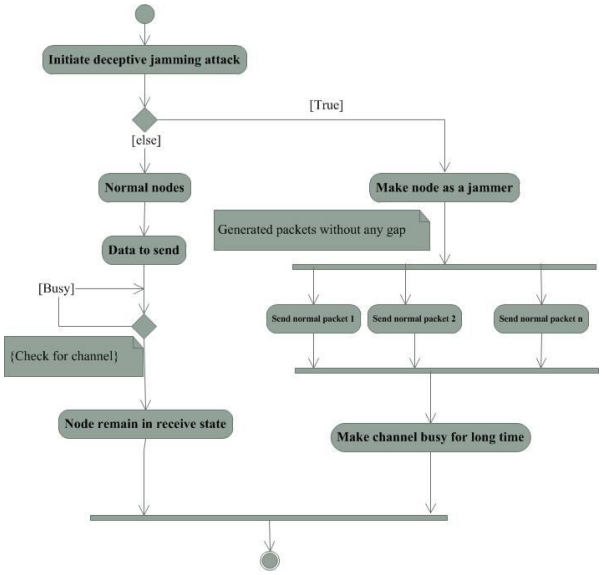

Figure 2: Activity modelling of deceptive jamming attack

Figure 2 shows the flow of activities in case of deceptive jamming attack. In case of deceptive jamming, attacker will take whole charge of channel by making the channel busy.

2.1.3 Random Jamming

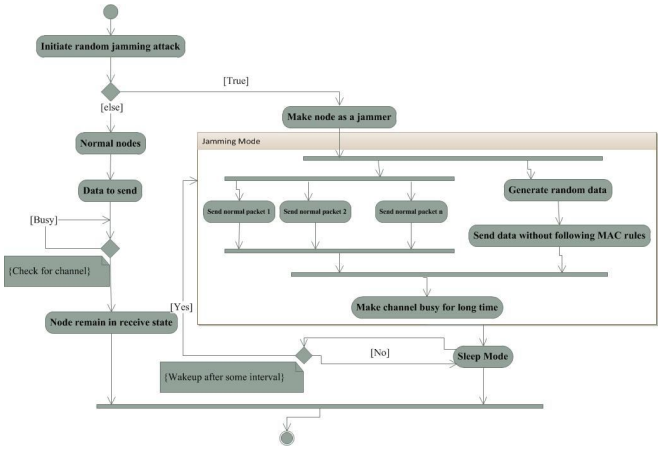

Figure 3: Activity modelling of random jamming attack

Figure 3 shows the different activities that takes place during the execution of random jamming attack. The random jamming attack is kind of intelligent attack where the jamming node thinks for saving of its own energy.

2.1.4 Reactive Jamming

Figure 4 shows the activity modelling of reactive jamming. It shows the execution steps of nodes in a network in case of reactive jamming.

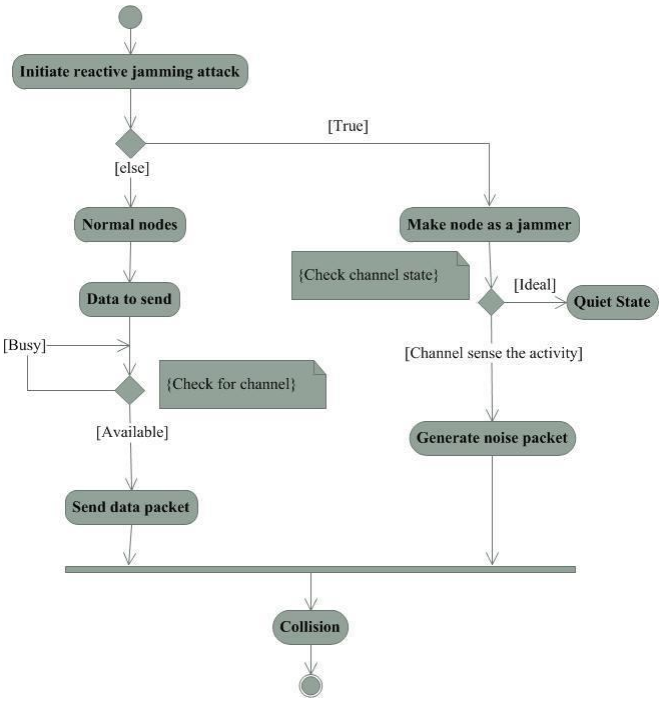

Figure 4: Activity modelling of reactive jamming attack

2.2.2 Sequential Modelling of Jamming Attack

The sequence diagram is used primarily to show the interactions between objects in the sequential order in which those interactions occur. The sequence diagram is also called as message sequence charts. A sequence diagram shows, as parallel vertical lines, the different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur.
It considers jamming attacker and different nodes in network as entities and interaction between them as the processes. It also considers normal behaviour of each node as, node transmit data after successful exchange of RTS and CTS. In each attack situation, external attacker initiates the attack on any of the node in the network and converts those nodes into malicious nodes, who are acting as a malicious node or jammer.

A. Constant Jamming Attack

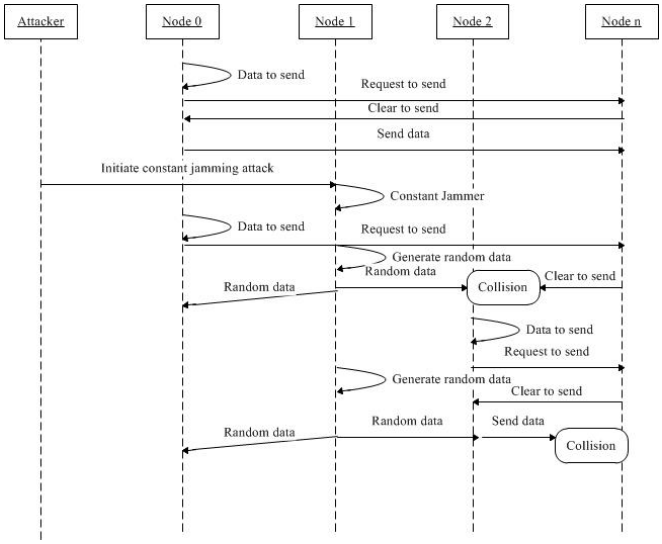

Figure 5: Sequential modelling of constant jamming attack

Figure 5 show the sequential modelling of constant jamming attack. It shows sequence of interaction between normal nodes, malicious nodes, and attacker.

B. Deceptive Jamming Attack

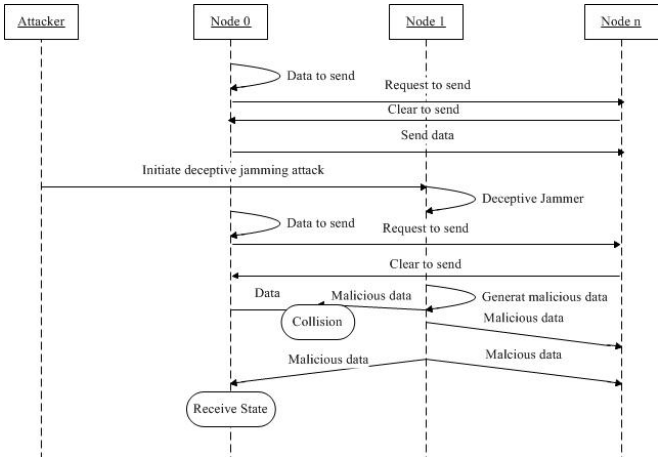

Figure 6: Sequential modelling of deceptive jamming attack

Figure 6 show the modelling of deceptive jamming attack using sequential modelling approach. Sequential modelling of deceptive jamming shows the different actions that take place on different objects (attacker and normal nodes) during execution of attack.

C. Random Jamming Attack

Figure 7 show the sequence of activities in case of random jamming attack.

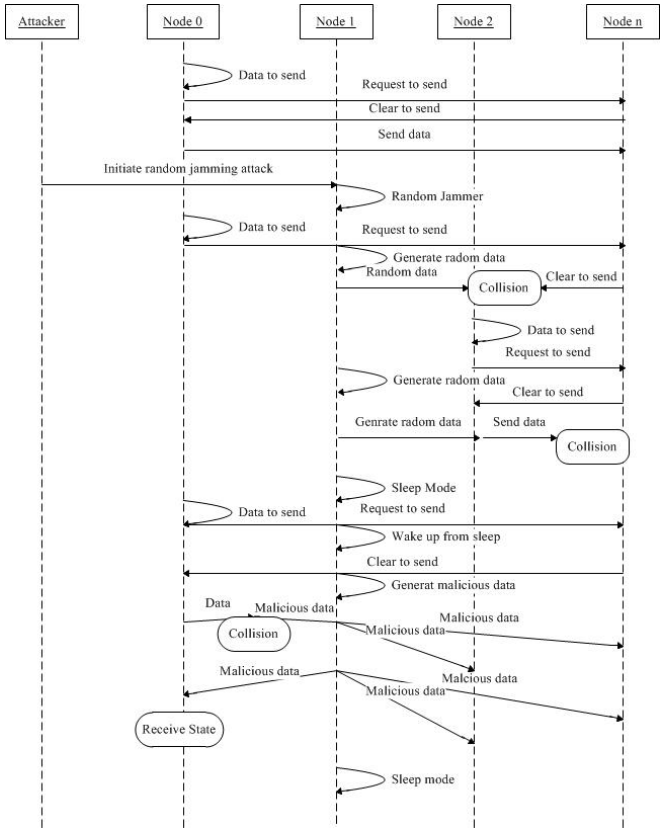

Figure 7: Sequential modelling of random jamming attack

D. Reactive Jamming Attack

Figure 8 show the sequential modelling of reactive jamming attack. reactive jamming attack is the most intelligent jamming attack which reacts in the network by observing the events in the network.

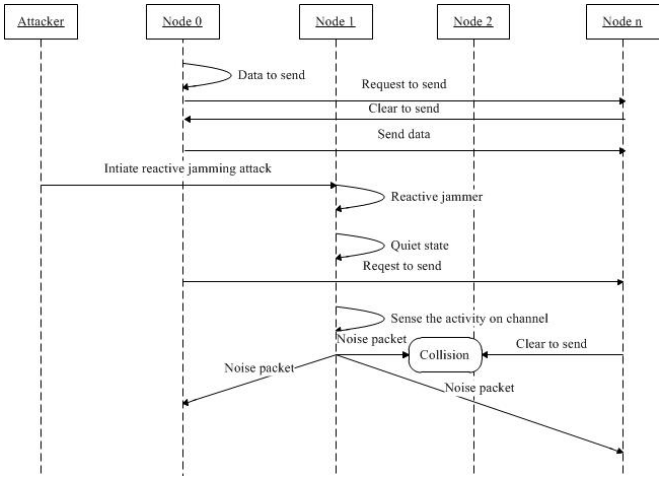

Figure 8: Sequential modelling of reactive jamming attack

III. PROPOSAL OF CLUSTER BASED JAMMING ATTACK

The previous sections of paper describe the jamming attack, its modelling and evaluation under network situations. The jamming considered in the previous sections and in literature is mainly for flat network, where the network is not divided into the parts. This kind of network is more prone to jamming as attack penetrates in faster way and destruct the network. The other kind of network is cluster-based network, where network is divided into small parts, called as clusters. Each cluster consists of CH, other nodes in cluster communicate with CH, and CH transmits the information to BS on behalf of other nodes. Cluster-based networks are scalable, having good energy efficiency and less prone to attack, as attack penetration limits to cluster. Therefore, more IoT applications preferred to use cluster-based network [7, 10]. These growing demands of cluster-based network lead to security loopholes in the system. Here, the section gives the details of possible reactive jamming attack named "Intelligent Cluster Head Attack" in cluster-based network and its evaluation to show how it is more destructive than other kind of jamming attacks.

3.1. Intelligent Cluster Head Jamming Attack

The attacker consider in this attack is intelligent attacker who can differentiate between the cluster head (CH) [11] and normal node in the network and continuously taking track of cluster head traffic. The main task of CH is to aggregate the information from normal nodes in the network and send it to the base station or other in between CH. Here, intelligent jammer initiates the attack whenever it detects some event on CH i.e. whenever CH is ready to transmit some aggregated data or receive some data from normal node. Once the jammer detects the event on CH it initiates the attack on CH and makes the CH as malicious CH. The all links in the network are considered to be bidirectional. The malicious CH can generate noise packets towards the BS or other CH and also towards the normal node in that cluster. The noise packets transmitted inside the cluster jam the traffic inside the cluster i.e. it jams the intra-cluster traffic and noise packets transmitted in between the CH jams the inter-cluster traffic. This way it creates the black hole in network which starts to eat whole network by producing malicious data.

3.2 Sequential modelling of Intelligent Cluster-Head Jamming Attack

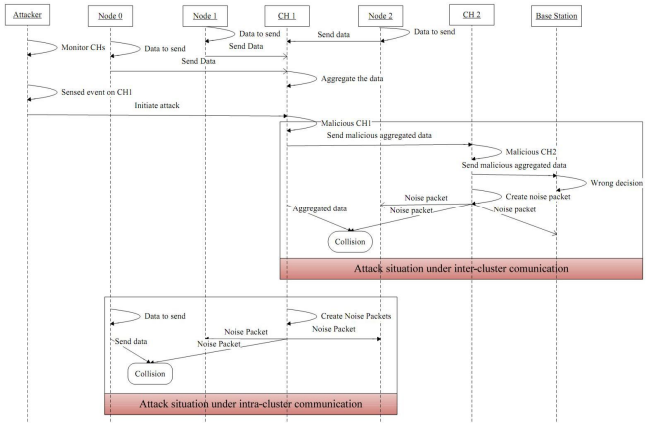

Figure 9: Sequential modelling of intelligent CH jamming attack

Figure 9 show the sequence of activities that happens during the deployment of intelligent CH jamming attack. The different activities are as follows,

- The attacker is continuously monitoring the traffic from the CH.
- Node 0, 1 and 2 have data to send and they will send it towards the CH, CH will aggregate the information and will try to send the data towards another CHs or BS.
- Whenever attacker senses the traffic on the CH it initiates the attack on CH1 and makes it malicious CH.
- Malicious CH1 send malicious aggregated data to other CHs and will try to make them malicious. This way it will make other CHs malicious by sending

malicious data towards them. Therefore, whatever data will reach to the BS will be the malicious and leads to wrong decision at BS.

- The malicious CHs can also send noise packet inside and outside the cluster. The aggregated data send outside the cluster and noise packet from malicious CH may collide, that leads to inter-cluster collision. The noise packet coming inside the cluster collides with normal data send by normal node and leads to intra-cluster collision.

3.3 Performance Impact of Intelligent CH Jamming Attack

The simulation uses same simulation parameters as shown in Table which was used in previous set of simulation of jamming attacks. The clustering algorithm used for formation of cluster is LEACH [12].

Table : Simulation Parameters

Parameter Name	Setting Used
Network Interface type	Wireless Physical:802.15.4
Radio Propagation Model	Two-Ray Ground
Antenna	Omni-directional antenna
Channel Type	Wireless Channel
Link Layer	Link Layer (LL)
Interface Queue	Priority Queue
Buffer size of IFq	50
MAC	802.15.4
Routing Protocol	Ad-hoc routing
Energy Model	EnergyModel
Initial Energy (initialEnergy_)	100J
Idle Power (idlePower_)	31mW
Receiving Power (rxPower_)	35mW
Transmission Power (txPower_)	31mW
Sleep Power (sleepPower_)	15µW
Number of nodes	100
Node Placement	Random

Figure 10, 11, and 12 shows the energy consumption, delay, and throughput respectively due to reactive jamming attack in cluster based network and intelligent CH jamming attack. The result of simulation shows that the energy consumption, delay, and reduction in throughput due to the intelligent CH jamming attack are more than reactive jamming attack. The main reason of reduction in performance in intelligent CH jamming attack is its intelligent behavior. It can make the differentiation of CH and normal node, and initiate its attack on CHs which jam the inter- and intra- cluster traffic and increase the total energy consumption, delay and reduce the throughput of the network.

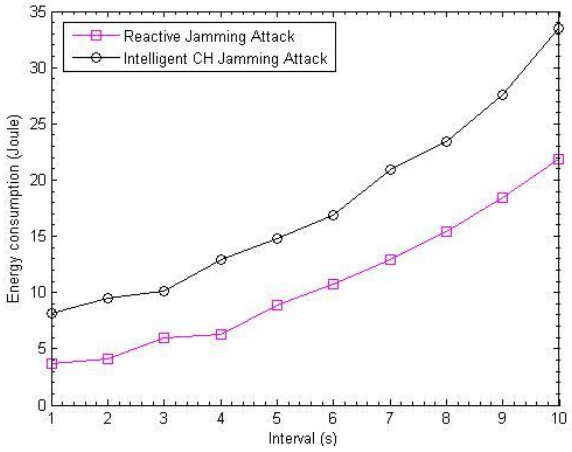

Figure 10: Comparative Energy consumption evaluation of reactive jamming attack with the proposed Intelligent CH jamming attack by varying the traffic interval

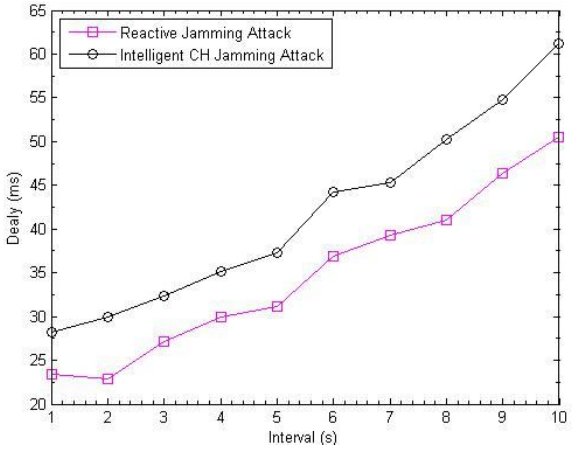

Figure 11: Comparative Delay evaluation of reactive jamming attack with the proposed Intelligent CH jamming attack by varying the traffic interval

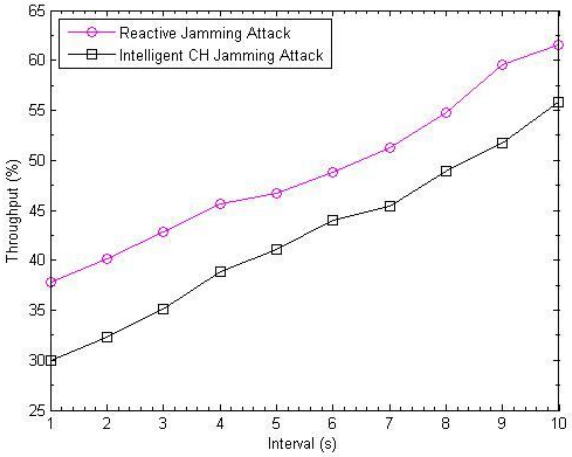

Figure 12: Comparative Throughput evaluation of reactive jamming attack with the proposed Intelligent CH jamming attack by varying the traffic interval

IV. REQUIREMENTS TO DESIGN EFFICIENT DEFENCE MECHANISM AGAINST JAMMING

Jamming attack can be deployed in system in many different ways and they are increasing as the WSN is getting more advanced. Therefore, to save the WSN from jamming, the defence mechanism should be developed by considering following requirements,

- Cross layer features like retransmitted RTS or DATA, failure of carrier sense, network allocator vector (NAV), etc. should be considered for detecting the attack efficiently because whenever jamming is deployed it changes the values of physical and MAC layer features.
- Nowadays most of the WSN deployments are made using cluster-based networks for improving energy efficiency and scalability. Therefore, it is necessary to develop defense mechanism by considering cluster-based networks.
- Use of threshold-based and game theoretic approach for developing efficient defence mechanism instead of traditional proactive and reactive development strategies.

V. CONCLUSIONS

The modelling of different jamming attack on WSN provides the functional view of sequence of activities executed during accomplishment of the jamming attack. The understanding of the activities will be useful tool to design efficient countermeasures for jamming attack. The experimental analysis of jamming attacks shows that reactive jamming is more difficult to detect than other attack because of its intelligent behaviour. The behavioural modelling and analysis of jamming attack is the useful tool to understand the behaviour of jamming attack and to develop the efficient defence strategy for WSN. The paper gives the new possibility of attack in cluster-based WSN i.e. intelligent CH jamming attack and shows that this attack jam the inter- and intra-cluster traffic which is more performance intensive than jamming because of reactive jammer. The understanding of modelling of attacks and its evaluation gives the guidelines and requirements to design the efficient jamming countermeasure.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee and DipakGhosal, "Wireless Sensor Networks: A survey", Elsevier Computer Networks, Vol. 52, Issue No. 12, pp. 2292–2330, 2011.

[2] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs", IEEE Communications Surveys & Tutorials, Vol. 11, Issue No.4, pp.42-56, 2012.

[3] A. R. Mahmood, H. H. Aly and M. N. El-Derini, "Defending against energy efficient link layer jamming denial of service attack in wireless sensor networks", IEEE AICCSA 27-30 December, Sharm El-Sheikh, Egypt, pp. 38-45, 2011.

[4] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defences", IEEE Journal on Pervasive Computing, Vol.7, Issue No.1, pp.74-81, 2015.

[5] T. Peder, "UML Bible", John Wiley & Sons, 2013.

[6] Wenyuan Xu, Ke Ma, Trappe W. andYanyong Zhang , "Jamming sensor networks: attack and defense strategies", IEEE Journal on Network, Vol.20, Issue No.3, pp. 41-47, 2016.

[7] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad and Ramjee Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)" Springer CNSA, 23- 25 July, Chennai, India, pp. 420-429, 2014.

[8] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori and Ramjee Prasad, "Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approch", River Publisher's Journal of Cyber Security and Mobility, Vol. 1, Issue No. 1, pp. 65-82, 2015.

[9] Derek J Corbett, Antonio G Ruzzelli, David Everitt, Gregory O'hare, "A Procedure for Benchmarking MAC Protocols used in Wireless Sensor Networks Technical Report 593", University of Sydeney, August 2006, pp. 1-28, 2006.

[10] Luigi Atzoria, Antonio Ierab, Giacomo Morabitoc, "The Internet of Things: A survey", Computer Network, Volume 54, Issue No. 15, pp. 2787–2805, 2016.

[11] Ammeer Ahmed Abbasi, Mohamed Younis, "A survey on clustering algorithms for wireless sensor network", Elsevier Computer Communication. Vol. 30, Issue No. 14-15, pp. 2826-2841, 2017.

[12] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, "Application specific protocol architecture for wireless microsensor networks", IEEE Transactions on Wireless Networking, Vol. 1, Issue 4, pp. 660-670, 2018.