Activity Modelling and Countermeasures on Jamming Attack

Sachin D. Babar, Neeli R. Prasad and Ramjee Prasad

Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark;
e-mail: {sdb, np, prasad}@es.aau.dk

Received 30 October 2012; Accepted 19 April 2013

Abstract

In last few decades, there has been a wide demand of wireless sensor networks (WSNs) in extensive mission critical applications such as monitoring, industrial control, military, health and many more. The larger demand of WSN in mission critical applications makes it more prone towards malicious users who are trying to invade. These security assaults worsen the performance of WSN in large extent in terms of energy consumption, throughput, and delay. Therefore, it is necessary to save the WSN from these attacks. The major aim of researchers working on WSN security is to enhance the performance of WSN in presence of these attacks. The major concentration of this paper is to model the behaviour of different kinds of jamming attacks using activity modelling and to find countermeasure against it. Jamming attack is the one of the ruinous invasion which blocks the channel by introducing larger amount of noise packets in a network. The activity modelling of jamming attack gives the perfect understanding of its accomplishment on WSN and it is useful to develop the security countermeasure against the attack.

This paper also gives the survey of different countermeasures of WSN and proposes the new countermeasure on jamming attack. The paper suggests the Threshold based Jamming Countermeasure (TJC) on reactive jamming attack which detects the jamming in network and save the network against reactive jamming attack. The implementation of proposed mechanism in different realistic conditions shows that TJC saves the network in case of reactive

Journal of Cyber Security and Mobility, Vol. 2, 1–27.

jamming attack with increased traffic and number of malicious nodes in a network. The paper simulate the TJC by considering the realistic scenarios which shows the adaptability of the algorithm in change traffic interval and mobility among the normal and malicious nodes.

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

1 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 of WSN are largely affected by security attacks which happen at various layers of WSN.

The main objective of this paper is to model the jamming attack [2, 3] which is one of the denials of service attack [4] which blocks the channel by introducing malicious traffic. 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 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.

The second objective is to analyse the different countermeasures on jamming attack. The literature survey shows that most of the solutions on jamming attack are hardware based which are quite expensive to implement and modify. The survey suggests that software based algorithm, which is quite efficient and cost effective way to stop the invasion of jamming attack. The researcher on jamming attack security did a major work for detecting the jamming attack and to reduce the effect of it on QoS of WSN by using some defensive strategies [6]. The defensive strategies can be useful to develop the efficient security model for Internet of Things (IoT) [7]. The task of making defensive strategies will be easier and efficient if we have the full understanding of behaviour of these attacks.

The last objective is to derive the efficient defence mechanism against jamming attack by understanding the behaviour of attacks and different available countermeasures. In this paper we propose a new countermeasure against reactive jamming, namely TJC. The TJC algorithm allows the attack into the network and starts its defensive mechanism once it detects the assaults in a network. It uses threshold based mechanism to detect the attack and to cure it. Here, every node maintains some send threshold value and it compares current transmission with threshold periodically. If it goes beyond that threshold, it understands that an attack has happened and then it applies defensive mechanism. It first detects the jamming node, then informs all neighbouring node about jammer node and change all paths coming from jammed node, i.e. it will put the jammer node out of network. The paper also simulates the TJC algorithm using Network Simulator (NS)-2 by considering realistic conditions. The simulation results show that TJC perform in better manner in existence of reactive jamming attack. It demonstrates good performance of TJC by varying traffic interval and number of malicious nodes in network. The major advantage of TJC is that its defensive mechanism supports with increased number of jamming nodes in a network.

The remaining part of the paper is organized as follows: Section 2 describes the different kinds of jamming attacks with activity modelling of constant jamming, deceptive jamming, random jamming and reactive jamming. Section 3 explains the various countermeasures on jamming detection and prevention. It also surveys widely used defensive mechanisms. Section 4 proposes the jamming countermeasure on reactive jamming attack based on threshold consideration. Section 5 describes the simulation environment for the TJC algorithm and also discusses the various results obtain in presence of reactive jamming. It also shows the comparative discussion of proposed algorithm. Finally, Section 6 concludes the paper with future work.

2 Proposed Activity Modelling of Jamming Attack

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. The next part of this section explains the activity modelling of four different kind of jamming attacks, i.e.

- Constant Jamming Attack
- Deceptive Jamming Attack
- Random Jamming Attack
- Reactive Jamming Attack

2.1 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. The sequences of activities are as follows:

- The attacker initiates the constant jamming attack. If attack is successful then node in a network will behave like a constant jammer and start to jam the network, otherwise node will do its regular activity.
- The normal node detects some event and tries to send the data to another node or destination. It checks for availability of channel, if channel is available then it will send data on the channel and send it towards the destination. If channel is not available then it will check for channel repeatedly after some particular interval.
- The jammer node generates the random data after some particular time interval and it will try to send the random data without following MAC rules i.e. without checking for channel.
- The random data generated from the jammer node may collide with data coming from normal node and it jams the whole traffic in the network by increasing the collision in network. The severity of constant jamming will be more if the interval between the random generations of data is too small.

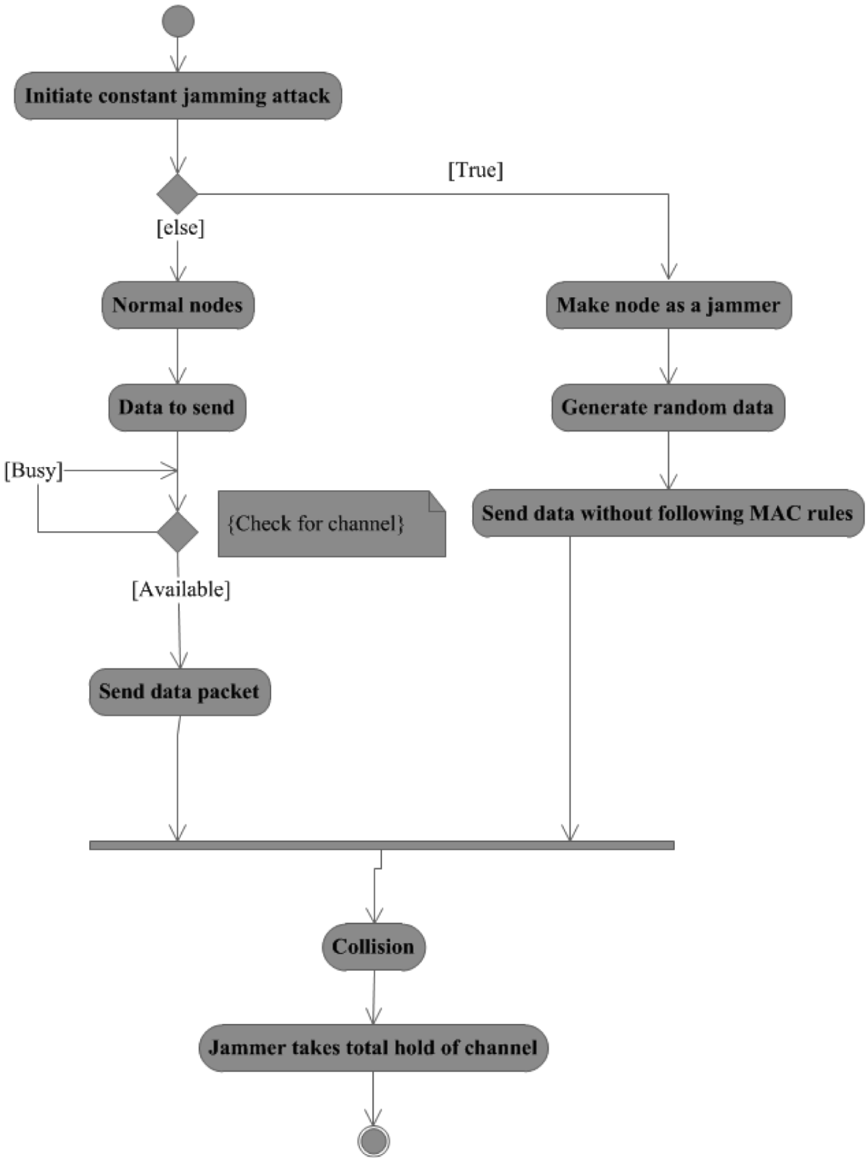

Figure 1 Activity modelling of constant jamming attack.

2.2 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. The different activities that happen during accomplishment of attack are as follows:

- The external attacker initiates the deceptive jamming attack on node in a network. If attack is successful the normal node will act like a deceptive jammer otherwise it will behave like a normal node.
- The normal node generates the data and tries to send the data towards the destination by checking the availability of channel.
- The jammer node generates the data packets continuously without keeping any time gap between the two packets. This continuous generation of packets put the channel in busy state for long time.
- The busy state of channel because of deceptive jamming keeps other normal node to be in receiving state. This behaviour of deceptive jamming increases the energy consumption, delay and decreases the total throughput of the network.

2.3 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. Therefore, it works in two modes, i.e. the jamming mode and the sleep mode. The details of execution of attack are as follows:

- If attack is successful, then the external attacker will initiate the attack by converting the normal node into jamming node.
- If channel is available, the normal node detects some event and tries to send the data packet towards another node or destination. The sender node checks for channel availability every time whenever it has data to send.
- The jammer node here works in two modes to save its energy and to last its effect for long time. In jamming mode it make channel busy either by continuously generating packet like deceptive jamming or generate random data after some specified interval without following MAC rules like constant jamming.
- The continuous block of channel by jammer node place the normal node in receive state for long time.

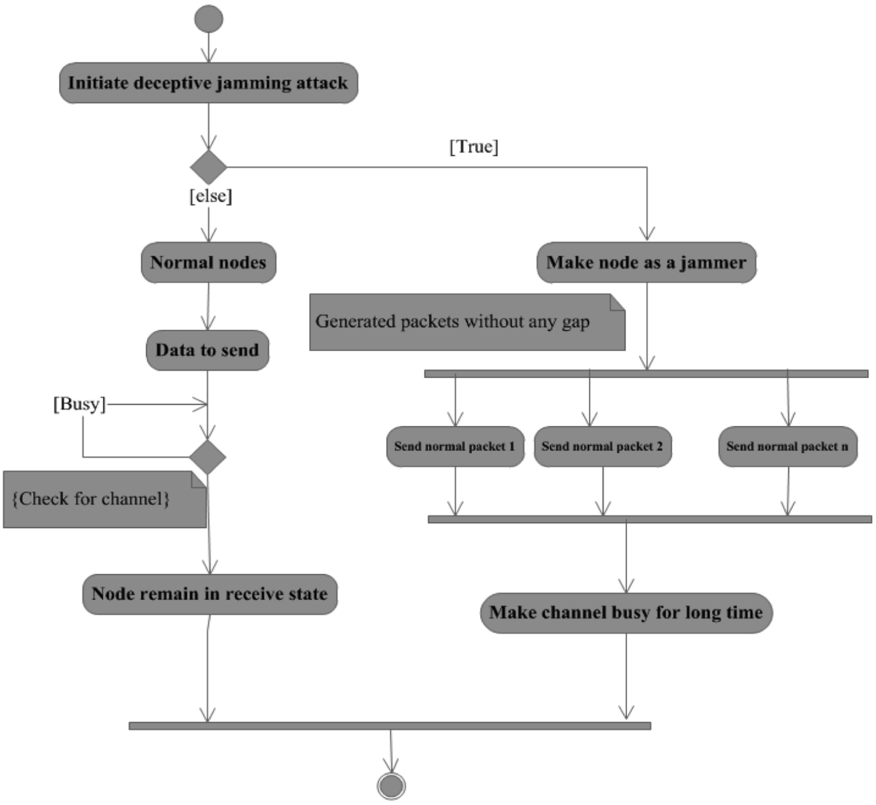

Figure 2 Activity modelling of deceptive jamming attack.

- The normal node changes its receiving state or can get the availability for some time whenever jammer node can go to sleep state. This behaviour of attack introduces the longer amount of delay in the transmission of data from the node.

2.4 Reactive Jamming Attack

Figure 4 shows the activity modelling of reactive jamming. It shows the execution steps of nodes in a network in case of reactive jamming. The steps are as follows:

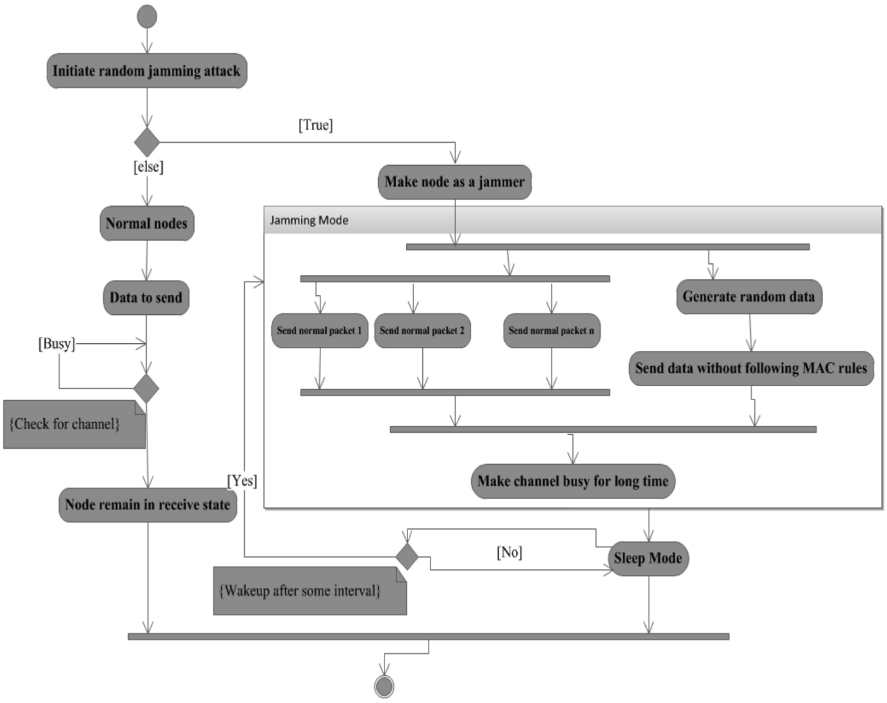

Figure 3 Activity modelling of random jamming attack.

- The reactive jamming attack is initiated by attacking on normal node, if it is successful then node will act like a reactive jammer, otherwise the normal node does its designated operations.
- The main feature of the attack is that it activates when other node in a network are busy to send data or if the channel is busy.
- Here, the normal node tries to send data towards the concern destination by checking the availability of channel and send the data on channel.
- The jammer node check for the channel if channel is ideal it will go to quiet state where it do nothing, else if channel is busy the jammer will activate and generate the noise packet continuously which results in collision in the network.
- The reactive jammer activate when the channel is busy. Therefore, it is very difficult to detect and reduce the effect of channel on performance of network.

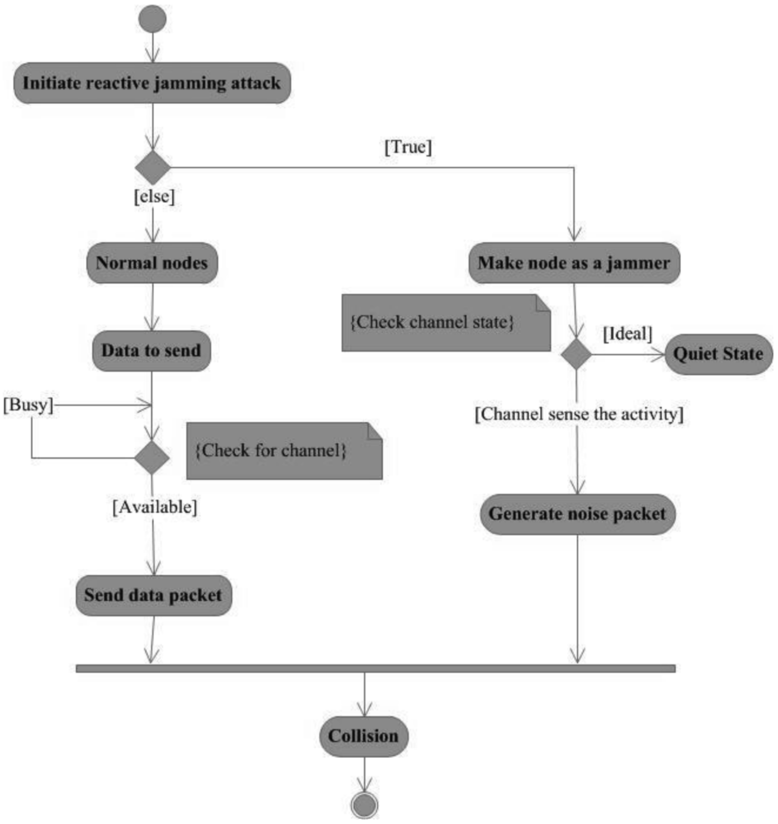

Figure 4 Activity modelling of reactive jamming attack.

3 Related Work on Countermeasures of Jamming Attacks

The security countermeasures against jamming attacks are mainly classified into [2]:

- Detection techniques.
- Proactive countermeasures.
- Reactive countermeasures.
- Mobile agent-based countermeasures.

Detection technique: The purpose of detection technique is to instantly detect jamming attacks. The approaches of these category cannot cope up with jamming alone; they can significantly enhance jamming protection only when used in conjunction with other countermeasures by providing valuable data.

Proactive countermeasures: The role of proactive countermeasures is to make the WSN immune to jamming attacks rather than reactively respond to such incidents. Proactive countermeasures can be classified in software i.e. algorithms for the detection of jamming or encryption of transmitted packets and combined software-hardware countermeasures.

Reactive countermeasures: The main characteristic of reactive countermeasures is that they enable reaction only upon the incident of a jamming attack, sensed by the WSN nodes. Reactive countermeasures can be further classified into software and combined software-hardware.

Mobile-agent based countermeasures: This class of anti-jamming approaches enables Mobile Agents (MAs) to enhance the survivability of WSNs. The term MA refers to an autonomous program with the ability to move from host to host and act on behalf of users towards the completion of an assigned task.

The survey in Table 1 shows the different countermeasures against jamming attack. The table compares all the countermeasures according to the type of technique, mechanism used, its energy efficiency, and implementation cost. The survey gives a varying concluding remark on each kind of countermeasure.

The detection techniques are less efficient according to total energy and implementation cost. Most of the detection technique cannot cope up with jamming attack individually; they require the support of some other countermeasures to work efficiently. The next kind of proactive mechanisms are better than the detection techniques by providing immunity solution to WSN against jamming attack. The proactive countermeasures are mainly classified into proactive software countermeasures and proactive software plus hardware countermeasures. The survey shows that proactive software countermeasure techniques are more efficient than other used techniques because they use some algorithm to defence from jamming instead of allowing the jamming. The proactive countermeasures are efficient solution for active jamming attack such as constant jamming, deceptive jamming and random jamming. The main disadvantage of proactive hardware plus software countermeasure is requirement of hardware, which increases its implementation cost.

The reactive countermeasure technique shows good performance than proactive one in case of reactive jamming attack. Reactive countermeasure allows the jamming in a network and react immediately after the detection of

Table 1 Survey of jamming attack countermeasures.

Countermeasures	*Type of technique*	*Mechanism*	*Energy efficiency*	*Implementation cost*
The feasibility of launching and detecting jamming attacks in WSNs [9]	Detection technique	It detects the jamming using signal strength or location information.	Low	Low
Radio interference detection protocol (RID) [10]	Detection technique	It uses the interference calculation method and information shared by the node.	Medium	High
Energy-efficient link-layer jamming attacks against WSN MAC protocols [11]	Proactive software	These techniques are mainly embedded inside the MAC to save from jamming effect. The techniques like high duty cycle, shorter data packets, encryption of link layer packet, TDMA protocol, and transmission in randomized interval are used to save from jamming.	Medium	Very low
Defeating energy-efficient jamming [12]	Proactive software	It used frame masking, frequency hopping, and packet fragmentation with redundant encoding.	High	Medium
Hemes II nodes [13]	Proactive hardware and software	It is special kind of node which uses hybrid FHSS-DSSS technique.	Medium	High
A jammed-area mapping service for sensor networks [14]	Reactive software	It detects the jamming by mapping the jam area.	Low	Medium
Channel surfing and spatial retreat [15]	Reactive hardware and software	It uses adaptive channel surfing techniques and spatial retreat mechanism.	High	High
Wormhole-based anti-jamming techniques in sensor networks [16]	Reactive hardware and software	It uses mechanisms like wired pair nodes, frequency hopping pairs with uncoordinated channel hopping.	Medium	High
Jamming attack detection and countermeasures in WSN using ant system [17]	Mobile agent	It used ant algorithm based mobility agent method.	Low	Medium
An algorithm for data fusion and jamming avoidance on WSNs [18]	Mobile agent	It used data fusion mechanism to reduce the effect of jamming and trying to avoid permanently.	Low	Medium
Optimal jamming attacks and network defence policies in wireless sensor networks [19]	Proactive software	Detect the jamming by analysing the percentage of collision and reduce the jamming effect by reducing the collision.	Low	Medium

jamming. They are also classified into reactive software and reactive software plus hardware countermeasures. Here, also reactive software approaches are much cost efficient and energy efficient than reactive hardware plus software countermeasures. The paper mainly concentrates on the software based reactive countermeasure against reactive jamming attack.

The last type of jamming countermeasure is mobile agent based countermeasures. It uses mobile agent who moves host to host to detect the jamming and to do the consigned task of counter measuring against jamming attack. The major disadvantage of this technique is its increase requirement of mobile agent in network, which effects in decreasing efficiency and increase in implementation cost and complexity.

4 Proposed Countermeasure on Reactive Jamming Attack

4.1 Network and Attacker Assumptions

- Network consists of n sensor nodes and one base station (BS).
- All nodes are connected together via bidirectional links.
- The nodes are equipped with synchronized clock, omni-directional antenna and two-ray ground propagation model. Each node is equipped with same capabilities.
- Nodes may communicate directly using single-hop communication or it may communicate using multi-hop communication.
- The nodes are distributed randomly in a network.
- Each sensor node periodically sends a message to the BS.
- The attack can be launch on any node in the network.
- The type of jamming attack assumed is reactive jamming attack, which will be activated when the jammer detects the activity on any node in the network.
- The jammer node is equipped same like a normal sensor node but with capability to generate random jamming signal (random messages).

4.2 Working Mechanism of Proposed Attack

In this paper we propose the threshold based jamming countermeasure (TJC). The key idea of algorithm is to enhance the performance of WSN in presence of reactive jamming attack and to save the WSN from harsh effects of reactive jamming. The algorithm saves the WSN by keeping some threshold at every node. The algorithm achieved it by introducing sending threshold which describe the maximum capabilities of node to send data.

The TJC algorithm works in two phases. The first phase in the threshold based jamming countermeasure is to decide the data sending threshold value of each node. The data sending threshold value is decided at BS side. Here, the BS has capabilities to count and maintain the record of the number of times data send from each node in WSN. Each node is sending the data towards the BS after regular interval, based on amount of data received from particular node per second during normal situation; BS decides the data sending threshold value of each node. BS will maintain the number of average send coming from each node as a sending threshold value.

In the second phase, algorithm will perform the check based on sending threshold value. Here, each node maintains the three states normal state, suspicious state and attacker state. The nodes in normal state are non-attacker node, suspicious state nodes are likely to be an attacker and attacker state nodes are jamming node that started to destroy the network. Initially all nodes are in normal state. The nodes are sending their information to BS either through one-hop or multi-hop way. If the BS is getting more data than expected, i.e. more than the consigned threshold value from the particular source node, then it is changing the state of node as suspicious state. The algorithm will do the path analysis for the suspicious state node; if the suspicious source node is the direct one-hop source then detection of attacker is easy just by doing one-hop path analysis. If the suspicious node is at multi-hop distance from BS then during path analysis phase, algorithm will check for individual node on path for its number of packet transmitted per second. If the number of packets generated by the nodes is more than the average send then that node is considered to be a jammer node and algorithm will make its state as jamming state. Once the jammer node will be detected then algorithm will remove the jammer node outside the path by changing the path through jamming node and also informed to the other neighbouring node to the network that, they have jammer node in neighbour. The detail flow of TJC algorithm is as shown in Figure 5.

5 Simulation of TJC Algorithm and Result Discussion

5.1 Implementation Details

The implementation of all attack is performed by using discrete event simulator NS-2. The parameters set during simulations are shown in Table 2. The idle power, receiving power, transmission power and sleep power are considered according to IEEE 802.15.4 radio model [20].

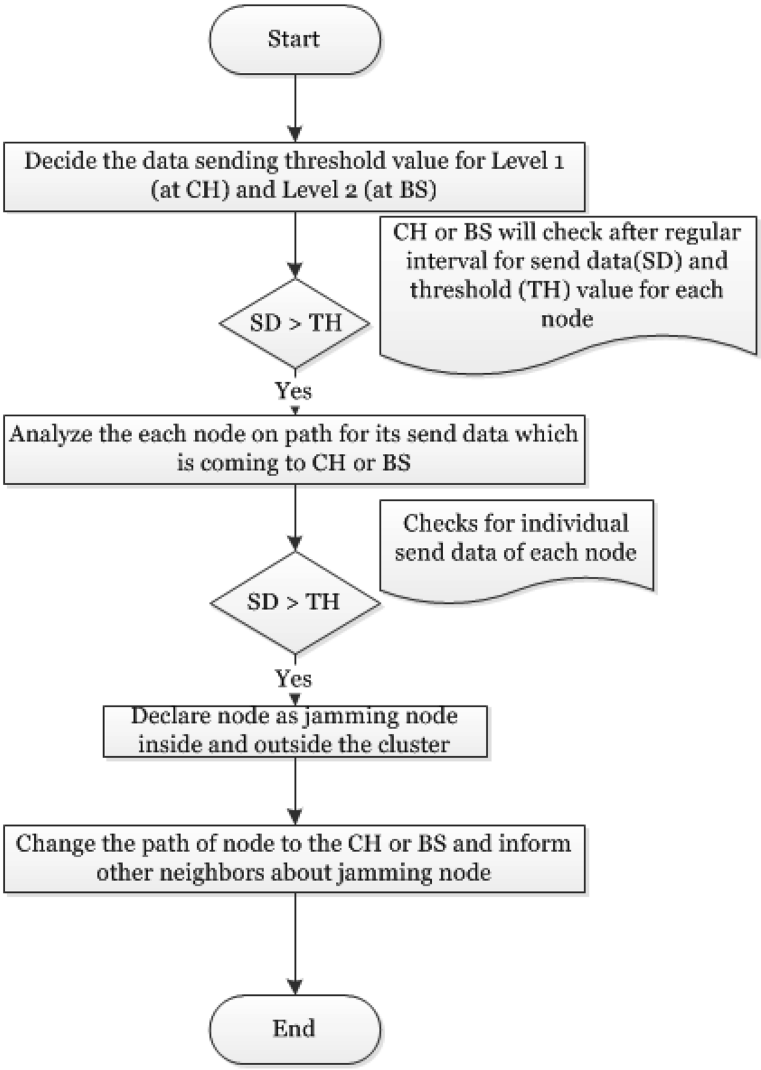
Start
Decide the data sending threshold value for Level 1 (at CH) and Level 2 (at BS)
CH or BS will check after regular interval for send data(SD) and threshold (TH) value for each node
SD > TH
Yes
Analyze the each node on path for its send data which is coming to CH or BS
Checks for individual send data of each node
SD > TH
Yes
Declare node as jamming node inside and outside the cluster
Change the path of node to the CH or BS and inform other neighbors about jamming node
End

Figure 5 Flow of TJC algorithm.

The simulations are performed in two different conditions. The different conditions are:

- WSN with reactive jamming attack
- WSN with reactive jamming attack with TJC countermeasure

The simulation of jamming attacks is done under following considerations:

- The simulation is performed by varying traffic interval, which is useful to measure the performance of attack and its countermeasures under various traffic conditions. The traffic interval varies from 1 to 10 s. The 1s traffic interval is consider as fast traffic and 10 s traffic interval is consider as slow traffic. These simulations consider number of malicious nodes in network or nodes under attack is one.
- The second set of simulation is performed by varying number of malicious nodes in the network. The number of malicious nodes in network considered is 1, 2, 4, 8 and 16. The traffic interval considers under this simulation is 1 s which is considered to be fast traffic in network. These set of simulations will be useful to analyse the effect of attack and its countermeasures by increasing the destructive entities in a network.
- The third set of simulation is performed by considering some realistic situations where each node is not transmitting information at same time and traffic interval consider is random traffic interval which varies in between 1 to 10 s randomly.
- The last set of simulation is performed by adding random mobility to all nodes in the network. The simulation considers the random traffic interval which varies in between 1 to 10 s randomly. The mobility speed consider here varies from 1 to 25 km/hr. This set of simulations gives the more realistic behaviour of the algorithm by considering random mobility and traffic interval.

5.2 Discussion of Results

5.2.1 Performance by varying traffic interval

Figures 6–8 show the measurement of average energy consumption, delay and throughput by varying the traffic interval respectively. The graphs show that the proposed algorithm TJC improves the energy consumption, delay, and throughput under reactive jamming attack conditions. The algorithm detects the jamming attack by analysing the network and reduces the effect of jamming attack by separating the jamming node from the network.

The energy consumption shown in Figure 6 is less after applying TJC algorithm than in the normal reactive jamming situation. The major reason for enhancing the energy efficiency in TJC is detection of reactive jammer and to place it out of the network. It will help to save the energy consumption happen due to reactive jamming attack.

Table 2 Simulation and node 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	Energy model
Initial energy (initialEnergy_)	100 J
Idle power (idlePower_)	31 mW
Receiving power (rxPower_)	35 mW
Transmission power (txPower_)	31 mW
Sleep power (sleepPower_)	15 μW
Number of nodes	100
Node placement	Random
Number of simulation runs	50

Figure 7 shows that the delay after applying TJC in a WSN is less than reactive jamming situation because TJC detects the jamming node in network and stop it by keeping it out of the network. The removal of jamming node helps to remove jam on channel, which gives the availability of channel to each node and helps in reduction of delay in case of TJC. In reactive jamming situation, which make channel busy for long time and incur a large waiting time for each node. The busy state of channel also effects on to the throughput of the network, which is improved after applying TJC algorithm as shown in Figure 8.

5.2.2 Performance by Varying Number of Malicious Nodes

Figures 9–11 describe the average energy consumption, delay, and throughput by changing the number of jamming nodes in the network. The number of jamming nodes in network increases from 1 to 16. The figures show that TJC algorithm improves performance against reactive jamming as the number of jamming nodes in network is increasing. The increasing number of jamming nodes in network gives more realistic analysis and adaptivity of TJC if amount of jamming is increasing in the network. The TJC shows efficiency by detecting the multiple jamming on the single path, which shows its perfection to cure the attack.

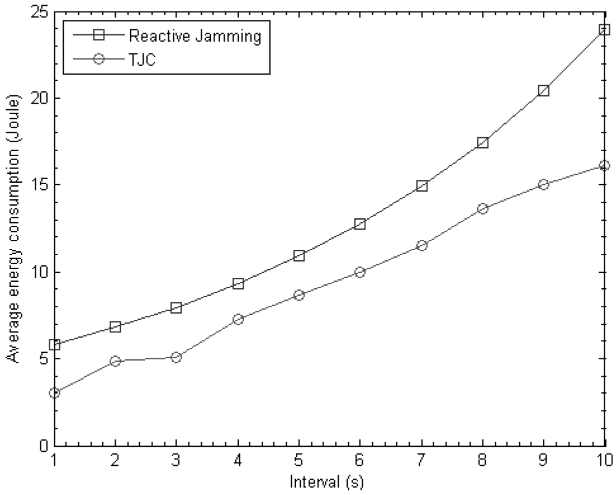

Figure 6 Average energy consumption vs. interval.

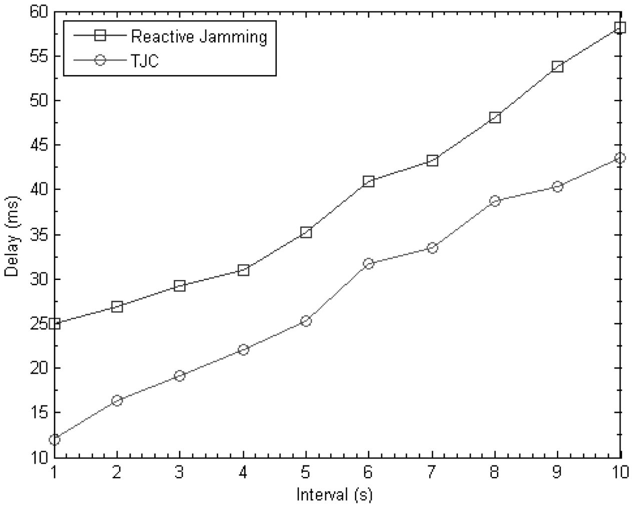

Figure 7 Delay vs. interval.

Figure 9 shows the average energy consumption by varying number of malicious nodes in a network, which shows TJC outperforms as number of malicious nodes is increasing. The major reason of energy saving in case of TJC is its jamming detection mechanism which helps to reduce the en-

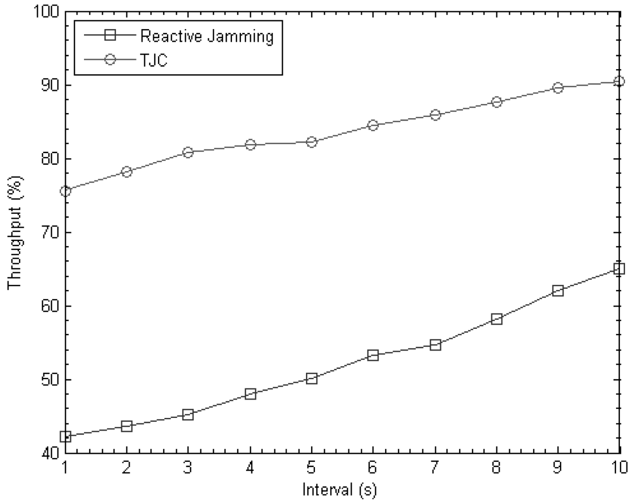

Figure 8 Throughput vs. interval.

ergy consumption due to jamming node and also helps to reduce the energy consumption due to active state of large number of nodes in WSN without sending any data to destination. The detection mechanism of TJC also helps to reduce delay and enhance throughput as shown in Figures 10 and 11. TJC reduce the delay by reducing the channel waiting time and increase throughput by giving quick channel availability to nodes in presence of reactive jamming.

5.2.3 Performance of TJC in Realistic Conditions

Figures 12–14 show the performance of TJC in more realistic situations such as by keeping random interval between the data packets and by transmitting data at different time instead of sending data at same time from each node. The realistic situation gives the more insight picture of performance of TJC in presence of reactive jamming attack. Figure 12 shows the average energy consumption of reactive jamming with and without TJC algorithm by varying number of malicious nodes. It shows that energy efficiency improves after applying TJC in realistic situations too because of technique it uses. The technique used by TJC helps to reduce delay and enhances the throughput as shown in Figures 13 and 14 respectively. The major reason of performance improvement in TJC is because of efficient channel availability compared to reactive jamming.

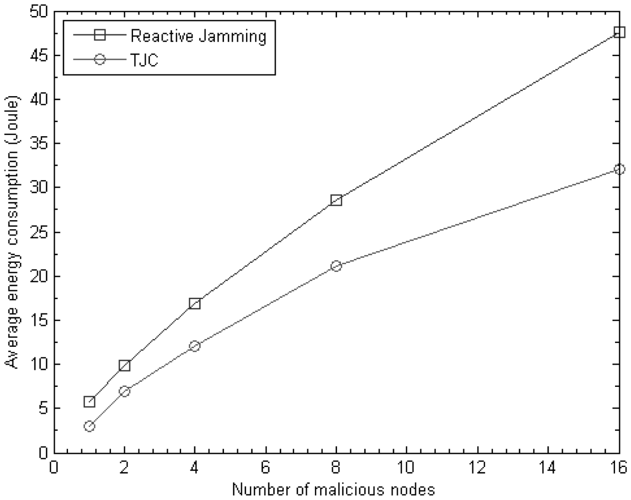

Figure 9 Average energy consumption vs. number of malicious nodes.

5.2.4 Performance of TJC by Considering Mobility

Figures 15–17 show the measurement of average-energy consumption, delay, and throughput respectively by varying the number of malicious nodes in the network. The result shown gives a more truthful support to the presented work because the measurement considers the random mobility among the nodes with random traffic interval. The mobility include in simulation consider the random waypoint mobility model [21]. The mobility scenario helps to check the adaptability of the concern countermeasure in presence of mobility among normal and malicious nodes.

The figures show that as the number of malicious nodes increases in the network, the average-energy consumption and delays also increase with it. The major reason of introducing higher energy consumption and delay is mobility. The mobility among the nodes will take more time to calculate the threshold values for each node, require more energy to scan the path and to detect the location of malicious and neighbouring nodes among it. These reasons lead to increase in energy consumption and delay, they also effects on to the reduction of throughput by increasing the time of jamming detection.

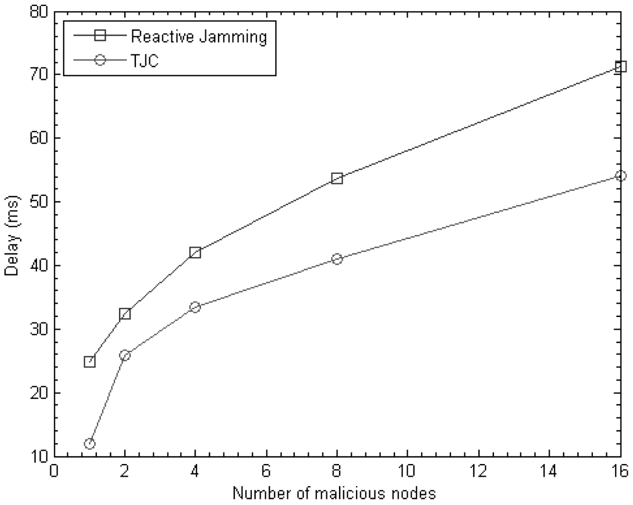

Figure 10 Delay vs. number of malicious nodes.

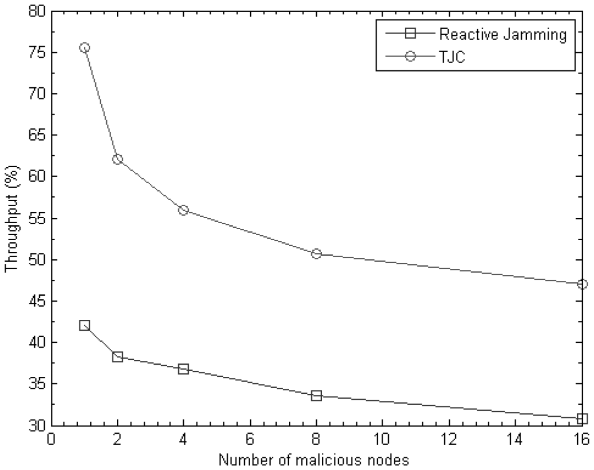

Figure 11 Throughput vs. number of malicious nodes.

6 Conclusions and Future Work

The activity modelling of different jamming attack on WSN provides the functional view of activities executed during accomplishment of the jamming attack. This knowledge is useful tool for the development of efficient security mechanism against jamming attacks. In this paper we also give a survey of

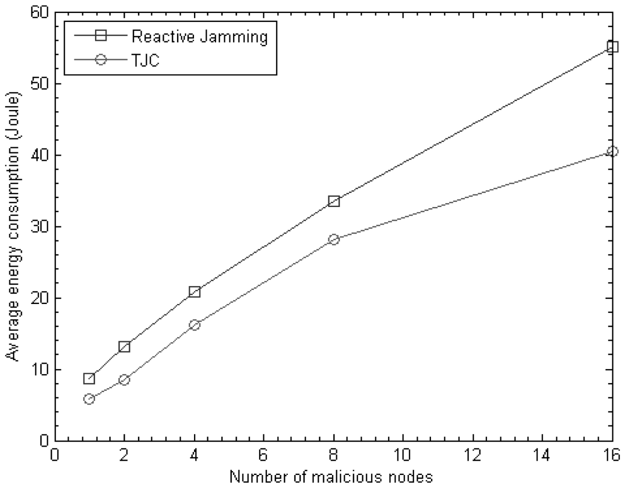

Figure 12 Average energy consumption vs. number of malicious nodes.

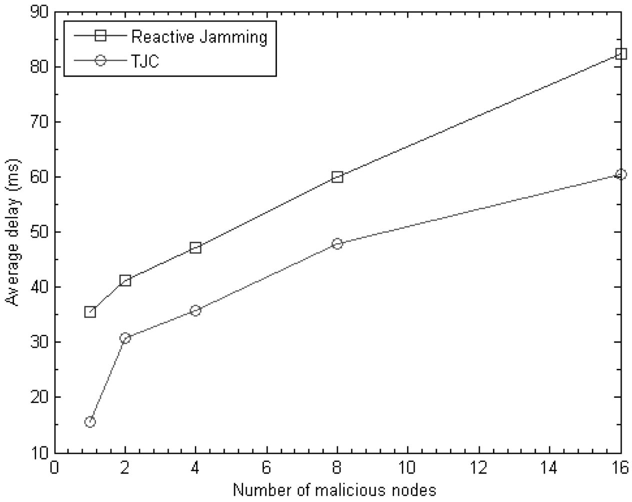

Figure 13 Average delays vs. number of malicious nodes.

existing countermeasures and proposes the countermeasure against reactive jamming attack. The paper proposes TJC countermeasure which shows good performance against reactive jamming attack with varying traffic interval and number of malicious nodes in a network. The proposed TJC algorithm is also tested by considering more realistic conditions where each node is not

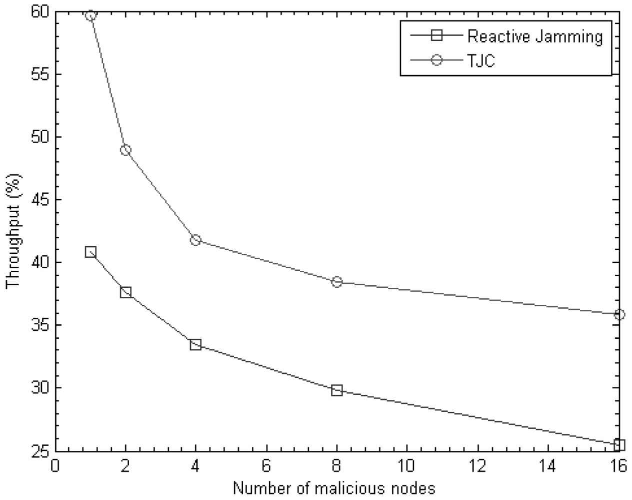

Figure 14 Throughput vs. number of malicious nodes.

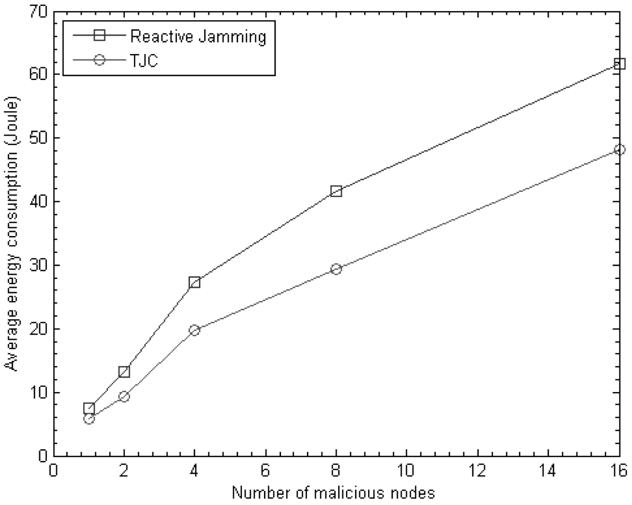

Figure 15 Average energy consumption vs. number of malicious nodes.

transmitting in particular time interval but nodes are transmitting at different time instance. The results under different conditions show that TJC is good solution against reactive jamming attack. The simulation of algorithm by considering mobility shows TJC adaptability with changing position of nodes in the network.

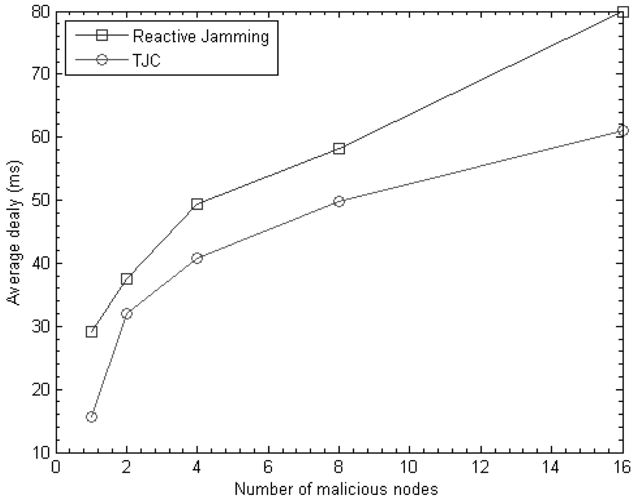

Figure 16 Average delays vs. number of malicious nodes.

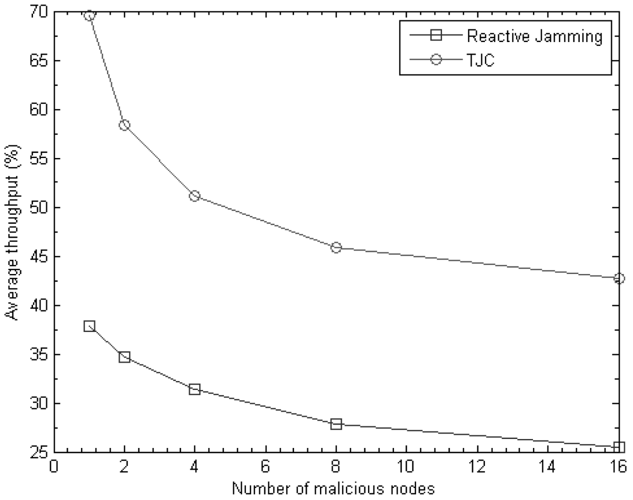

Figure 17 Average throughput vs. number of malicious nodes.

In future research will concentrate on finding a more efficient solution against other kind of jamming attacks by considering the mobility effects. The proposed TJC algorithm can also be extended for cluster based network by distributing task of threshold calculation among the cluster heads (CHs) to save the network from normal reactive jamming and intelligent CH reactive jamming.

References

[1] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor networks: A survey. Elsevier Computer Networks, 52(12):2292–2330, 2008.

[2] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou. A survey on jamming attacks and countermeasures in WSNs. IEEE Communications Surveys & Tutorials, 11(4):42–56, 2009.

[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. In Proceedings of IEEE AICCSA, Sharm El-Sheikh, Egypt, 27–30 December, 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, 7(1):74–81, 2008.

[5] T. Peder, UML Bible. John Wiley & Sons, 2003.

[6] Wenyuan Xu, Ke Ma, W. Trappe, and Yanyong Zhang. Jamming sensor networks: attack and defense strategies. IEEE Journal on Networks, 20(3):41–47, 2006.

[7] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. Proposed security model and threat taxonomy for the Internet of Things (IoT). In Springer CNSA, Chennai, India, 23–25 July, pp. 420–429, 2010.

[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 approach. Journal of Cyber Security and Mobility, 1(1):65–82, 2012.

[9] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings ACM MobiHoc, Urbana Champaign, IL, 25–28 May, pp. 46–57, 2005.

[10] G. Zhou, T. He, J.A. Stankovic, and T. Abdelzaher. RID: Radio interference detection in wireless sensor networks. In Proceedings IEEE INFOCOM, Miami, FL, 13–17 March, pp. 891–901, 2005.

[11] Y. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. ACM Transaction on Sensor Network, 5(1):6.1–6.38, 2009.

[12] A.D. Wood, J.A. Stankovic, and Gang Zhou. DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. In Proceedings IEEE SECON, San Diego, CA, 18–21 June, pp.60–69, 2007.

[13] A. Mpitziopoulos, D. Gavalas, G. Pantziou, and C. Konstantopoulos. Defending wireless sensor nhetworks from jamming attacks. In Proceedings IEEE PIMRC, Athens, Greece, 3–7 September, pp. 1–5, 2007.

[14] A.D. Wood, J.A. Stankovic, and S.H. Son. JAM: A jammed-area mapping service for sensor networks. In Proceedings IEEE RTSS, Cancun, Mexico, 3–5 December, pp. 286–297, 2003.

[15] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: Defenses against wireless denial of service. In Proceedings ACM Workshop on Wireless Security, New York, 26 September–1 October, pp. 80–89, 2004.

[16] M. Cagalj, S. Capkun, and J.P. Hubaux, Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[17] Rajani Muraleedharan and Lisa Osadciw. Jamming attack detection and countermeasures in wireless sensor network using ant system. In Proceedings SPIE, Orlando, FL, 12 March, pp. 1–5, 2006.

[18] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou. JAID: An algorithm for data fusion and jamming avoidance on distributed sensor networks. Elsevier Journal of Pervasive and Mobile Computing, 5(2):135–147, 2006.

[19] Mingyan Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attack strategies and network defense policies in wireless sensor networks. IEEE Transactions on Mobile Computing, 9(8):1119–1133, 2010.

[20] Derek J. Corbett, Antonio G. Ruzzelli, David Everitt, and Gregory O'Hare. A procedure for benchmarking MAC protocols used in wireless sensor networks. Technical Report 593, School of IT, University of Sydney, pp. 1–28, August 2006.

[21] C. Bettstetter, G. Resta, and P. Santi. The node distribution of the random waypoint mobility model for wireless ad hoc networks. IEEE Transactions on Mobile Computing, 2(3):257–269, 2003.

Biographies

Sachin D. Babar is ISTE Life Member. He is graduated in Computer Engineering from Pune University, Maharashtra, India in 2002 and received Master in Computer Engineering from Pune University, Maharashtra, India in 2006. From 2002 to 2003, he was working as lecturer in D.Y. Patil College of Engineering, Pune, India. From 2003 to 2004, he was working as lecturer in Bharati Vidyapeeth College of Engineering, Pune, India. From 2005 to 2006, he was working as lecturer in Rajarshi Shahu College of Engineering, Pune, India. From July 2006, he has been working as an Assistant Professor in Department of Information Technology, STES's Sinhgad Institute of Technology, Lonavala, India. Currently he is pursuing his Ph.D. in Wireless Communication at Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark. He has published 20 papers at national and international levels. He has authored two books on subjects like Software Engineering and Analysis of Algorithm & Design. He has received the Cambridge International Certificate for Teachers and Trainers at Professional level under MISSION10X Program. He is IBM DB2 certified professional. His research interests are Data Structures, Algorithms, Theory of Computer Science, IoT and Security.

Neeli Rashmi Prasad, Ph.D., IEEE Senior Member, Director, Center For TeleInfrastructure USA (CTIF-USA), Princeton, USA. She is also Head of Research and Coordinator of Themantic area Network without Borders, Center for TeleInfrastruktur (CTIF) headoffice, Aalborg University, Aalborg, Denmark.

She is leading IoT Testbed at Easy Life Lab (IoT/M2M and eHealth) and Secure Cognitive radio network testbed at S-Cogito Lab (Network Management, Security, Planning , etc.). She received her Ph.D. from University of Rome "Tor Vergata", Rome, Italy, in the field of "adaptive security for wireless heterogeneous networks" in 2004 and M.Sc. (Ir.) degree in Electrical Engineering from Delft University of Technology, the Netherlands, in the field of "Indoor Wireless Communications using Slotted ISMA Protocols" in 1997.

She has over 15 years of management and research experience both in industry and academia. She has gained a large and strong experience into the administrative and project coordination of EU-funded and Industrial research projects. She joined Libertel (now Vodafone NL), The Netherlands in 1997. Until May 2001, she worked at Wireless LANs in Wireless Communications and Networking Division of Lucent Technologie, the Netherlands. From June 2001 to July 2003, she was with T-Mobile Netherlands, the Netherlands. Subsequently, from July 2003 to April 2004, at PCOM:I3, Aalborg, Denmark. She has been involved in a number of EU-funded R&D projects, including FP7 CP Betaas for M2M & Cloud, FP7 IP ISISEMD ICt for Demetia, FP7 IP ASPIRE RFID and Middleware, FP7 IP FUTON Wired-Wireless Convergence, FP6 IP eSENSE WSNs, FP6 NoE CRUISE WSNs, FP6 IP MAGNET and FP6 IP Magnet Beyond Secure Personal Networks/Future Internet as the latest ones. She is currently the project coordinator of the FP7 CIP-PSP LIFE 2.0 and IST IP ASPIRE and was project coordinator of FP6 NoE CRUISE. She was also the leader of EC Cluster for Mesh and Sensor Networks and is Counselor of IEEE Student Branch, Aalborg. Her current research interests are in the area of IoT & M2M, Cloud, identity management, mobility and network management; practical radio resource management; security, privacy and trust. Experience in other fields includes physical layer techniques, policy based management, short-range communications. She has published over 160 publications ranging from top journals, international conferences and chapters in books. She is and has been in the organization and TPC member of several international conferences. She is the co-editor is chief of *Journal for Cyber Security and Mobility* by River Publishers and associate editor of *Social Media and Social Networking* by Springer.

Ramjee Prasad (R) is currently the Director of the Center for TeleInfrastruktur (CTIF) at Aalborg University (AAU), Denmark and Professor, Wireless Information Multimedia Communication Chair. He is the Founding Chairman of the Global ICT Standardisation Forum for India (GISFI: www.gisfi.org) established in 2009. GISFI has the purpose of increasing the collaboration between European, Indian, Japanese, North-American, and other worldwide standardization activities in the area of Information and Communication Technology (ICT) and related application areas. He was the Founding Chairman of the HERMES Partnership – a network of leading independent European research centres established in 1997, of which he is now the Honorary Chair.

Ramjee Prasad is the founding editor-in-chief of the Springer *International Journal on Wireless Personal Communications*. He is a member of the editorial board of several other renowned international journals, including those of River Publishers. He is a member of the Steering, Advisory, and Technical Program committees of many renowned annual international conferences, including Wireless Personal Multimedia Communications Symposium (WPMC) and Wireless VITAE. He is a Fellow of the Institute of Electrical and Electronic Engineers (IEEE), USA, the Institution of Electronics and Telecommunications Engineers (IETE), India, the Institution of Engineering and Technology (IET), UK, and a member of the Netherlands Electronics and Radio Society (NERG) and the Danish Engineering Society (IDA). He is also a Knight ("Ridder") of the Order of Dannebrog (2010), a distinguishment awarded by the Queen of Denmark.