International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A SECURE AND DISTRIBUTED DYNAMIC SOLUTION TO SELECTIVE JAMMING ATTACK IN TDMA USING RSA WITH MULTI-CHANNEL WSNs

Pooja N. Ause[1],P.I.Basarkod[2]

[1,2]*School of Electronics and Communication Engineering,REVA University, Bangalore, (India)*

ABSTRACT

In wireless sensor network (WSN) often uses time division multiple access (TDMA) especially for critical applications, as it provides high energy proficiency, definite bandwidth, restricted and predictable latency, and nonexistence of collision. During wireless transmission, the integrity information of data packets can be obtained by RSA algorithm. Here, we adopted the multichannel technique for reducing the transmission delay. In TDMA transmission, slots are usually pre-allocated to sensor nodes, and each slot is used by the same node for a number of consecutive super frames, and because of this TDMA is helpless due to selective jamming attack. A victim's node can be ruined by jamming its slot by an opponent; such attack turns to be energy efficient, effective and very complex to identify. This paper is aimed at changing the slot utilization pattern at every super frame and this is done by JAMMY, thus fickle to the opponent. JAMMY isn't brought together, as sensor nodes decide the following opening usage design in a disseminated and self-ruling way. From the performance analysis, result obtained shows that Jammy introduces negligible overhead yet allows numerous nodes to join network, in a limited number of super frames.

Keywords: *RSA algorithm, TDMA, Super frames, JAMMY.*

I.INTRODUCTION

Wireless Sensor Networks (WSNs) are being utilized in an assortment of areas including modern applications, industrial facility robotization, natural and wellbeing checking and basic foundations. In such applications, to access the shared wireless medium Time Division Multiple Access (TDMA) is used. In TDMA, super frames are developed by dividing time, each super frames comprising of a fixed number of transmission slot. To make each sensors node to be active during its slots, the slots are assigned to sensor nodes, while it can sleep for the rest of the time[1]. It is realised that TDMA provides highenergy proficiency, definite bandwidth, restricted and predictable latency, and nonexistence of collision.

Unfortunately, TDMA suffers from selective jamming attacks, a particularly insidious form of Denial-of Service(DoS) that allows an opponent could preliminarily monitor communication of a victim node with a very low probability to be detected. In TDMA based WSNs nodes commonly hold its opening for some back to back

super frames. In this manner, an opponent could preliminarily monitor communication screen correspondence and recognize the slot of the victim node. Then, the opponent could jam that slot feigning a collision and sleep for the rest of super frame. [2]Such an attack is very effective, energy efficient, and much more difficult to be detected than a traditional wide-band jamming . [3][6]Although a few stratergies are accessible for jamming identification, their applications to specific jamming is incredibly complicated by the constrained introduction time of the opponent and the limited amount of traffic affected by the attack. Both physical layer solutions and cyber countermeasures against selective jamming have been proposed in the literature, but they all exhibit some limitations. For example, solutions operating at physical layer rely on spread-spectrum techniques, increased transmission power, and antenna polarization or directional transmission. Unfortunately, they only make the attack more difficult but are not able to neutralize it.

Furthermore,[5] these solutions are more suitable for military networks with a large design space, whereas commercial networks do not have the same flexibility, since they must confirm to norms and laws. Cyber countermeasures for WSNs include. However, they are mainly tailored to the IEEE 802.15.4 standard and, hence, are thus introduces a significant computing and communication overhead. Finally, is a totally centralised solution, where sensor nodes regularly exchange messages with a coordinator node and hence displays a considerable energy consumption. [4]To beat these limitations, We propose JAMMY, a conveyed and dynamic arrangement against particular jamming attacks in TDMA based WSNs. The proposed strategy depends on a key thought, haphazardly per-quieting the opening usage design on a super frame premise. By doing so, the slot(s) used by a sensor node change(s) unpredictably at each super frame.

II.LITERATURE SURVEY

Farhana Ashrafet. al [1] proposes “Bankrupting the Jammer in WSN”. The high defenseless of the remote sensor nodes to jamming emerges from the low flexibility and easy differentiability of protocol control messages, and the high expectedness of node wakeup schedules. This paper aims at, Jam-Buster a Jam-resistant solution for WSN, orthogonal to the existing anti jamming solutions, by using equal size packets and multi-block payloads increases flexibility and reduces expectedness by randomizing the wakeup times of the sensors. Jam- resilient system is obtained by the arrangement of the three components that forces the jammer to transmit more enabling faster detection of the jammer by the sensor, and to spend more energy to effective and reduce its own lifetime.

Mario et. al [2] proposes “Wormhole-Based Anti-jamming Techniques in Sensor Networks” Due to their very nature, being the category of wireless network, wireless sensor networks are most open to “radio channel jamming” based Denial-of-Service (DOS) attacks. An opponent can easily mask the events that the sensor network should detect by stealthily Jamming an appropriate subset of the nodes in this way, they can foil reporting to the network operator regarding what they are sensing. Therefore, even if an event is sensed by one or several nodes, the network operator cannot be informed on time. This shows how the sensor nodes can exploit channel diversity in order to create wormholes that lead out of the jammed region, through which an

alarm can be transmitted to the network operator. We propose three solutions: the first is based on wired pairs of sensors, the second relies on frequency hopping, and the third is based on a novel concept called uncoordinated channel hopping.

Radosvetaet. al [3] "On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack". In the last several years IEEE 802.15.4 has been accepted as a major MAC layer protocol for wireless sensor networks (WSNs) and has attracted the interest of the research community associated with security issues as the expanded scope of use situations with security issues as the expanded scope of use situations bring out new conceivable outcomes for abuse and taking uncalled for preferred standpoint of sensor hubs and their activity. As these nodes are very resource restrained such possible attacks and their early detection must be carefully considered. This paper overviews the known strikes on remote sensor networks, recognizes and explores another strikes on remote sensor networks, recognizes and explores another strikes, Guaranteed Time slot(GTS) attack, taking as a premise the IEEE 802.15.4 MAC

Zhuo Lu et. al [4] "Modelling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications" Recently, wireless networking for emerging cyber-physical systems, in particular the smart grid, has been drawing increasing attention in that it has broad applications for time-critical message delivery among electronic devices on physical infrastructures. However, the shared nature of wireless channels unavoidably exposes the messages in transit to jamming attacks, which broadcast radio interference to affect the networks, where communication traffic is more time-critical than that in conventional data-service networks, such as cellular and Wi-Fi networks. In this paper, we aim at modelling and detecting jamming attacks against time-critical wireless networks with applications to the smart grid.

In contrast to communication networks where packets-oriented metrics, such as packet loss and throughput are used to measure.The network performance, we introduce a new metric, message invalidation ratio, to quantify the performance of time- critical applications. Our modelling approach is inspired by the similarity between the behaviour of a jammer who attempts to disrupt the delivery of a time-critical message and the behaviour of a gambler who intends to win a gambling game. Therefore, by gambling- based modelling and real-time experiments, we find that there exists a phase transition phenomenon for successful time-critical message delivery under a variety of jamming attacks.

Hossenet. al [5] "Jmming-Resilent Multipath Routing" Reliability of wireless communication is effected to due to the Jamming attacks, as they can effectively disrupt communication between any node pairs. The primarily focus of existing jamming defences is on repairing connectivity between adjacent nodes. In this paper, through multipath routing address jamming at the network level and focus on restoring the end-to-end data delivery. As long as all paths do not fail concurrently, the end-to-end path availability is maintained. Prior work in multipath selection improves routing availability by choosing node disjointees paths or link-disjoint paths. However, through our experiments on jamming effects using Micaz nodes, we show that disjointees is insufficient for

selecting fault-independent paths. Thus, we address multipath selection based on the knowledge of a path's availability history, Using Availability History Vectors (AHVs) of paths, we present a centralised AHV based algorithm to select fault-independent paths, and a distributed AHV-based routing protocol built on top of a classic routing algorithm in adhoc networks.

Proan et.al [6] "Packet-Hiding Methods for Preventing Selective Jamming Attacks" The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically refered to as jamming. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of- Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this wireless networks. In these attacks, the adversary is active only for a short period of a time, selectively targeting messages of high importance.

III. PROPOSED SYSTEM

With this method a mechanism is being created which prevents the jamming attacks on the wireless networks. The RSA algorithms and multichannel wireless sensor networks helps in examining the detection of jamming attacks and its efficiency along with the communication overhead of the networks. RSA passes scrambled shared keys for symmetric key cryptography which thusly can perform mass encryption-unscrambling tasks at significantly higher speed. The key idea on which the methodology was projected is random permutation of the slot utilization pattern over a super frame basis.

By doing so, the slot(s) used by a sensor node change(s) unpredictably at each super frame. RSA algorithm is used for providing data packets integrity information during wireless transmission. Through simulation and performance analysis, the implemented provides higher packet delivery ratio. Hence, the adversary is compelled to jam slots picked at random in the hope to guess the ones used by the victim node. With the assumption that at each super frame a single slot per sensor is considered, so the probability obtained of each successful selective jamming attack would be N=1,(N is taken as number of super frame). JAMMY is distributed, as each sensor node computes the slot to use in the next super frame autonomously (i.e., without exchanging data) and in a consistent way (i.e., without causing collisions). JAMMY is also dynamic as it manages dynamic join and leave of multiple nodes. Finally, JAMMY is general as, in principle, it can be used in any TDMA network.

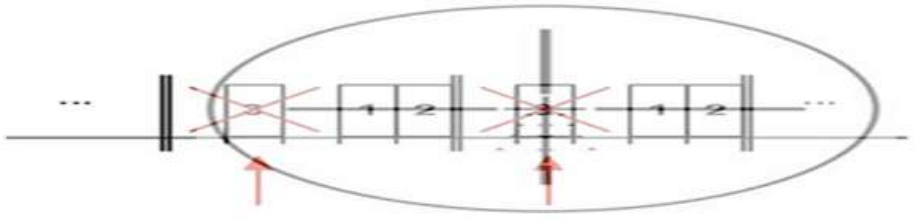

Fig.1. Selective Jamming

IV. RESULTS

The aim of proposed paper is achieved by the following parameters. The parameters are mentioned below:

- Packet delivery ratio

PDR=R/T

PDR= No .of Received packets/Total No .of Packet sent

Figure 2 illustrates the packet delivery ratio result generated and compared with other existing proposals.

- Throughput

Th=No. of Bits Received/simulation Time in Ms

Th= Bits/Ms

- Packet Drop

P.D=Total no. of packet sent-Total No. of packet Received

- Energy consumption

Consumption=Total energy-Remaining energy

C=T-R

Figure 2 illustrates the packet delivery ratio, Figure 3 illustrates the throughput, Figure 4 shows the packet drop, Figure5 shows the energy consumption, the results generated and compared with other existing proposals. The proposed system results are better than existing system. In graph green line isexisting proposal, red line is proposed system.

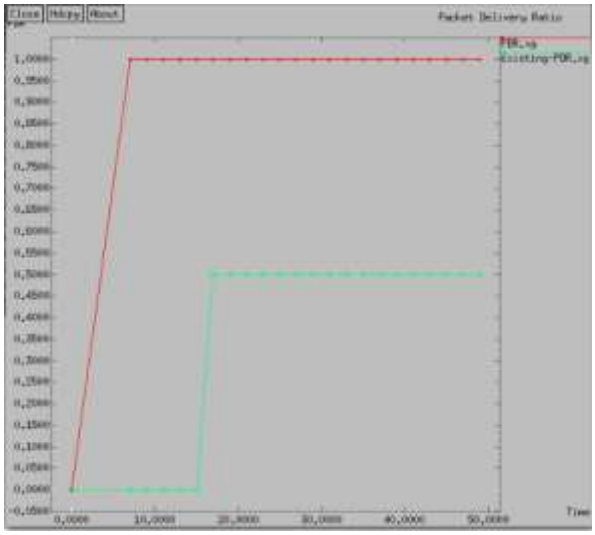

Fig.2. Packet delivery ratio

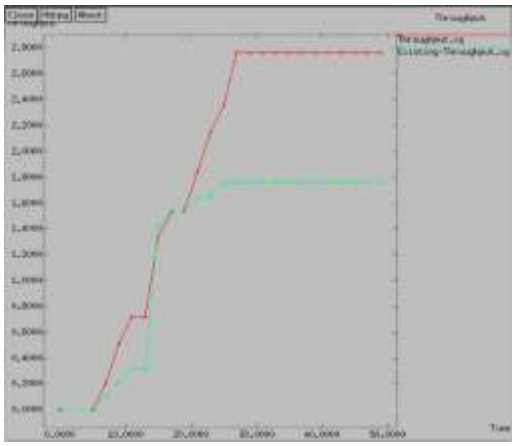

Fig.3.Throughput

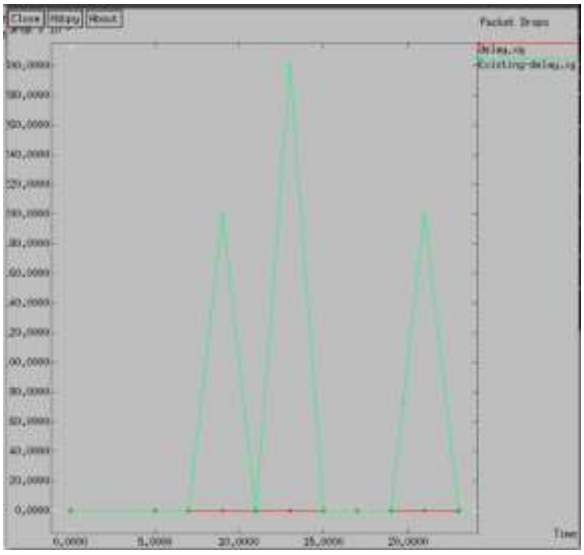

Fig.4.Packet drop

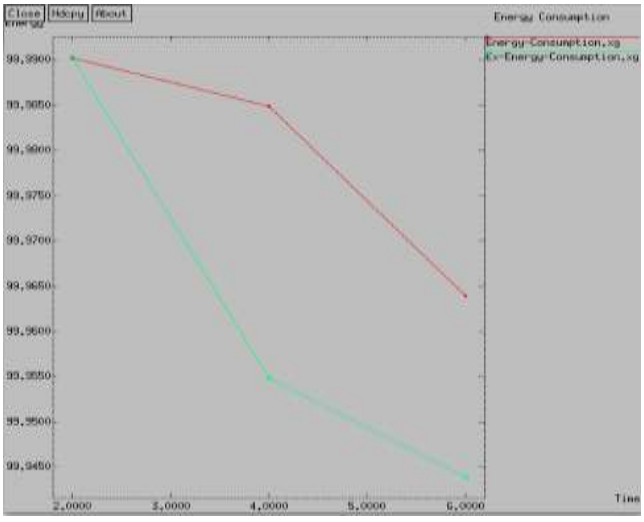

Fig.5. Energy consumption

The above parameters shows comparison between existing system and proposed system.FigureFrom the parameters mentioned above when PDR is higher then throughput is also higher and vice versa. There can be numerous exceptions for instance, let say a packet is send from source to destination, we get a error and is re-transmitted. In one case it get effectively re-transmitted, while in second case it get re-transmitted in tenth attempt. Here throughput in both the cases would be same.

When one or more packets of Data travelling across a Wireless Sensor Network fails to reach the destination a Packet loss is encountered. The main reason for Packet loss is due to error in data transmission across Wireless Sensor Network or due to network congestion. The energy consumed during the process, and the Energy Consumption is calculated.

V. CONCLUSION

JAMMY is a dispersed answer for specific jamming attacks in TDMA WSNs. JAMMY powers the opponent to play out the attacks aimlessly, henceforth diminishing its adequacy and have accessed JAMMY through examination, recreation, and estimations in a genuine substantial scale test bed. It is possible to send large amount of Data on Multi-Channel but large amount of data is not possible to send on a Single-Channel. As per the security concern for the data that is being transmitted encryption is done.

REFERENCES

[1]Farhana Ashraf, Yih-Chun Hu and Robin H. Kravets, Bankrupting the Jammer in WSN,978-1-4673-2433-5/12/$31.00 ©2012 IEEE.

[2] Mario, Cagalj, Srdjan , Capkun, and Jean-Pierre Hubaux ,Wormhole-Based Anti jamming Techniques in Sensor Networks,Ieee transactions on mobile computing, vol. 6, no. 1, january 2007.

[3] Radosveta Sokullu1, Orhan Dagdeviren2, Ilker Korkmaz3,On the IEEE 802.15.4 MAC Layer Attacks: GTS Attack, The Second International Conference on Sensor Technologies and Applications ,ieeedoi 10.1109/sensorcomm.2008.75.

[4] Zhuo Lu, Wenye Wang, and Cliff Wang, Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications, ieee transactions on mobile computing, vol. 13, no. 8, august 2014

[5] Hossen Mustafa, Xin Zhang, Zhenhua Liu, Jamming-Resilient Multipath Routing, ieee transactions on dependable and secure computing, vol. 9, no. 6, november/december 2012

[6] Alejandro Proan˜o and LoukasLazos , Packet-Hiding Methods for Preventing Selective Jamming Attacks**,** ieee communications surveys & tutorials, vol. 11, no. 4, fourth quarter 2009

[7] T. Shu, M. Krunz, and S. Vrudhula,"Power balanced coverage-time optimization for clustered wireless sensor networks," in Proc. ACM MobiHoc, 2005, pp. 111–120.

[8] T. Shu and M. Krunz, "Coverage-time optimization for clustered wireless sensor networks: A power-balancing approach," IEEE/ACM Trans. Netw., vol. 18, no. 1, pp. 202–215, Feb. 2010.

[9] K. A. Darabkh et al., "Performance evaluation of selective and adaptive heads clustering algorithms over wireless sensor networks," J. Netw.Comput. Appl., vol. 35, no. 6, pp. 2068–2080, Nov. 2012.

[10] W. K. Lai, C. S. Fan, and L. Y. Lin, "Arranging cluster sizes and transmission ranges for wireless sensor networks," Inf. Sci., vol. 183, no. 1, pp. 117–131, Jan. 2012.