

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES
A DEALT AND EFFECTIVE SOLUTION TO DISCRIMINATING JAMMING ATTACK
IN TDMA WSNs

Vinay S¹, Rajesh K S², Prathibha Shankar S³ & Meghana B⁴

^{1,3,4}UG student, Dept. of CSE, RRCE Bangalore, ² Associate Professor, Dept. of CSE, RRCE Bangalore

ABSTRACT

WSNs stands for wireless sensor network and TDMA stands for time division multiple access are used in the WSNs. TDMA is widely used in critical applications because of its high energy efficiency and its bandwidth and due to its non-collision of the nodes in the network. But however TDMA is boon even they have limitations. It is easy for the selective jamming in the sensor nodes the slots are allocated previously and slots are used by the same nodes for upcoming superframes. Easily it can be blocked by jamming the slots. Hence it is very difficult to identify where the slot has been jammed and it is difficult to detect. So in this proposed system we are going to present a JAMMI, A dealt and effective solution to discriminating jamming attack in TDMA WSNs. JAMMI changes the slot using patterns and making it difficult for the hacker. It is decentralized because the slot uses the pattern in the different way.

Keywords: WSN, TDMA, jamming attacks.

I. INTRODUCTION

Wireless sensor networks (WSNs) are widely depleted in a ramification of domain names along with its vast application in the industrial field and infrastructure field. Wireless sensor networks (wsn) consist of a collection of nodes which might be deployed randomly in a antagonistic surroundings. it have a set infrastructure and self-prepared in to a arbitrary topology. Although there are improvements in generation, safety in WSN is an essential situation. As the deployed sensors are in open surroundings, the intrusion of assaults may be very a great deal higher. Additionally the WSN has broadcast nature of communique; they're effortlessly suffering from the assaults. Common attacks are the DOS, Sybil attack, spoofing and many more types of attack.

There are 4 types of jamming attack can occur proactive jammers, reactive jammers, constant jammer and the random jammer. The different type of jamming detection techniques are WSN using time stamp, fuzzy based technique, using wavelets, by intelligent bivariate k-means technique, in our method we are using TDMA technique.

In such packages, time division multiple accesses (TDMA) is frequently used to get admission to the shared wireless medium. In TDMA, time is split into a chain of periodic superframes, every consisting of a hard and fast variety of transmission slots. Ordinarily, spaces are allotted to sensor hubs with the end goal that every hub should be enthusiastic best all through its own slot(s), while it can rest for whatever remains of the time. It's far perceived that TDMA bears ensured transmission capacity, over the top quality productivity, nonappearance of impacts notwithstanding limited and unsurprising inactivity. Unfortunately, TDMA experiences particular sticking assault, a particularly guileful type of dissent of-benefit (dos) that allows a foe to totally ruin the discussion of a casualty hub with an absolutely low probability to be distinguished. In TDMA -essentially based WSNs, a hub for the most part holds its opening for some continuous superframes. Therefore, an enemy may need to begin with show correspondence and run over the space of the casualty hub.

In the proposed system data is sent through wireless medium. In this system TDMA technique is used. Using random slots data is transmitted. Fisher-Yates algorithm is used for the generating the random slots.

II. RELATED WORK

Jamming represent is the one of the important threats in the wireless sensor networks. The authors Aristides Mpitiopoulos et al. [1] proposed the critical issues of jamming and covers the related works regarding jamming. They overview about the communication protocol used in the WSN and characteristics of contemporary WSNs. They provide the countermeasures against the jamming attack, analysis are measured and defenses against the jamming attacks are given.

Next survey paper deals with the Denial of sleep threats and countermeasures, here measures are taken to save the energy of the nodes in the networks. This is proposed by the David R. Raymond, Scott F. Midkiff [2] they completely explore the details of the denial of sleep attack, which would intentionally target the sensors in the network. Jamming attacks are very harmful to the wireless communication they can easily disrupt communication between two pair of nodes this was proposed by the Hossen Mustafa, Xin Zhang[4]. They address jamming at the network level and try to restore end to end data delivery through multipathing. Selecting multipath improves routing availability. They uses AHV(availability history vectors) based algorithm to select fault independent paths. These are effective to overcome the jamming attack. WSNs are built upon shared medium it would be easy for the hacker to analyze the radio interface or jamming or dos attack. In this paper by Wenyuan Xu et al.[3] they insisted 2 phase strategy includes diagnosis of attack and defense strategy. Their aim is to achieve communication in presence of jammer. Availability of service in wireless network depends on the ability for network users to establish and maintain communication channels using control messages from base stations and other users. The hacker with knowledge of communication protocol can establish a efficient DOS attack. Patrick[5] and team proposes a frame work for control channel access scheme using random assignments of keys to hide the control channel. They proposed the algorithm called GUIDE for identification of compromised user in the system based on the control channel that is jammed. Various design trade-offs between robustness to control channel jamming and resource expenditure.

The current framework It requires that the whole parcel, including the header, is encoded (it is a typical practice to leave the header decoded, with the goal that collectors can early prematurely end the gathering of bundles not bound to them).The focal Coordinator speaks to a solitary purpose of disappointment. The goal of a consistent jammer is to degenerate all system parcels, by persistently transmitting arbitrary signs. JAMMI is additionally unique as it oversees dynamic join and leave of various hubs. At last, JAMMI is general as, on a fundamental level, it can be utilized as a part of any TDMA network. In TDMA transmission, spaces are designated already to sensor hubs and each opening is utilized by a similar hub for various back to back superframes. The proposed framework JAMMI changes the space use design at each superframe, consequently making it conflicting to the programmer. The two segments of JAMMI, are irregular stage calculation and Secure Pseudo-Random Number Generator. JAMMI enables sensor hubs to join the system. In extra to it various hubs can join the system in the meantime by executing a particular join technique. The join method acknowledges that each joining hub would execute a Slot Acquisition calculation to get an opening in the superframe for information transmission. Join Manager can be made out of an arrangement of copies, every last one of which holds both the present stage key and secure pseudo-irregular number generator state. Keeps itself synchronized with superframes to keep up an up and coming estimation of the SPRNG state. Takes an interest to rekeying if there should arise an occurrence of hub's clearing out.

III. SYSTEM ARCHITECTURE

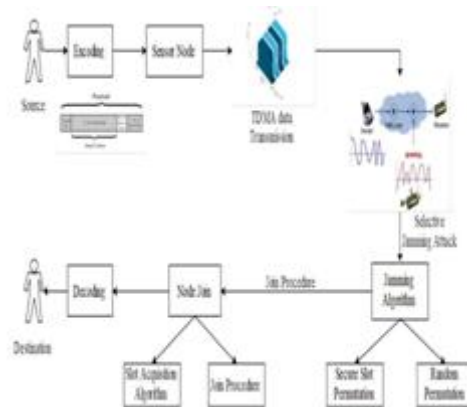


Fig1: system architecture of a proposed system

The system architecture is as shown in the figure1. Here the source is the sender and destination is the receiver. In wireless sensor network it's difficult to send the data from one side to another side we may face n number of problems one of the main problem is jamming attack, the intruder tries to takes the data in between the communication channel. In our proposed model we are trying to avoid the jamming attack by introducing the jamming algorithms and basic cryptographic algorithm.

Early, the source is going to send the data packets first we have to make sure the data is in encrypted form for that going to use AES algorithm. Using this AES algorithm data packets are encoded. Now the packets are not in readable from as they are not in plain text they are in cipher text formats. We are using the Time Division Multiple Access for transmission the data from one node to another node in WSN's. Using this method of transmission we can able to send the packets in different time slots. So that the intruder cannot be able to determine at which time the packet is sent. If the jamming attack happens means the data in the encrypted form will be taken off, there is a chance of data is lost so to control that jamming algorithms are introduced. In this proposed method there are 2 types of jamming algorithm one Random Permutation and another one is secure slot permutation algorithm JAMMI enables sensor hubs to join the system whenever. Likewise, various hubs can join the system in the meantime by executing a particular join strategy. The join methodology expects that each joining hubs utilize an opening procurement calculation. At that point the information bundle at last got by the decoder which would unscramble it back to plain content and it would achieve the goal.

IV. MODULES

Module is a logical separation of functionality within a project. We can have as many modules in an application, they are basically used for reusability and better code maintenance. In this paper there are 4 modules they are Trusted Central Authority certification for the node, Mapping to 1-Factorization Method for nodes, Sequential Unicast Mode for Single Hop broadcast, Assisted Broadcast Mode for Single Hop broadcast.



Fig2: Trusted Central Authority certification for the node

Figure 2 represents TCA certification for node. Every node has to register their details to central networks authority in Wireless network message

In transmission process central network authority is considered as the genuine person. Nodes have to be registered with all its information and verify it. The central authority would generate the authentication certification by providing it with the unique id and saves all the details in the database of the server.

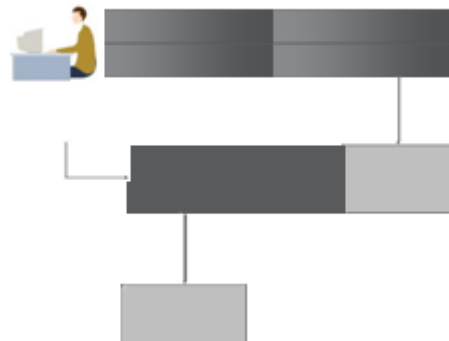


Fig 3: Mapping to 1-factorization

Figure 3 shows the mapping to 1-factorisation technique, first count of the number of edges in network and call it as ϵ . number of edges is $\epsilon=2n-1$

2. $2n$ represents the total number of nodes. According to the F_{2n} every node has to meet all the remaining nodes, then assign the frequencies using the splitting algorithm for time slot i .

Figure4 shows the sequential unicast mode, based on the distance between the receiver and the sender data will be broadcast with different frequencies [7]. Broadcasted data is received by the nodes from single user using sequential unicast mode algorithm.



Fig4: Sequential unicast mode



Fig 5 Assisted broadcast mode

Figure 5 represents assisted broadcast mode directly the sender sends the data to the different neighbor with some frequencies [7]. After data is received it should be sent it to the neighbors. This solves the problem of using different frequency signals and reusable of signals.

V. UML REPRESENTATION



Fig 6 Use case diagram of proposed system

The fig 6 diagram represents the use case diagram. Here the node 1 refers to the user and node2 refers to the trusted central authority. The user will be having the accessible to the TCA certification generation, node authentication and the mode selection. In mode selection selected in 2 ways one is sequential broadcast mode and assisted broadcast mode. Node2 i.e. trusted central authority would help to set the node location and mode selection. Trusted central authority will also analyze the network and it also allots the slots in the respective nodes.

Sequence diagram of the paper is as shown in the figure7. There are 4 entities in the sequence diagram they are node, central trusted authority, 1-factorisation method, broadcast mode. First node has to be registered, central trust authority generates the key, node would be given the location meanwhile the central trusted authority will analyze the network and 1-factorisation technique is implemented. Central trusted authority will check for the broadcast mode. Broadcast mode is selected and finally data is broadcasted and data is received by the receiver.

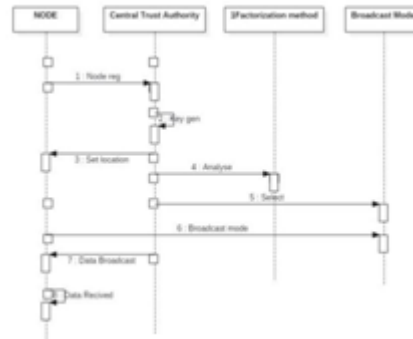


Fig 7 Sequence diagram of proposed system

VI. ALGORITHMS

Advance encryption is also called as AES algorithm. AES algorithm is the most used and the popular algorithm in the recent times, it is first adopted by the US military and it is popular almost all over the globe and it supersedes the DES algorithm.

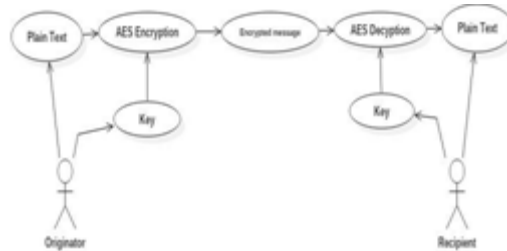


Fig 8 component of AES algorithm

A single block of 128 bit plain text is taken as input. The plain text is taken 16bytes m_0-m_{15} in the initialization stage. Each byte is substituted for a different byte. The rows are shifted in permutation style. The columns are mixed in mixcolumn stage. After this an exclusive OR operation is performed using 128bit keys.

To detect the jamming attack here we are going to use the 2 algorithms one is random number permutation algorithm and another is secure slot permutation algorithm. To generate the random numbers we are going to use the fisher-yates algorithm.

Fisher-Yates algorithm is used for the generating the random permutation. These are the steps to be followed for generating the random permutation. First write down the numbers from 1-N, then select i such that it is in the number generated. Let j be the random number generator. Swap the value i and j and finally repeat it again.

Code for the above algorithm is shown below:

```

for(i from n-1) down to 1
do
{

```

$j \leftarrow$ random number $0 \leq j \leq i$

swap $a[i], a[j]$

}

Let $C(a,b)$ denote a cipher text, it would encrypt a plain text b with the help of key a . encryption key E would be the generator.

Consider a counter it would be initialized to 'c'.

Initially the counter would be c_0 .

Let the sequence be $c, c+1, c+2, C+3, \dots$ and so

on. When we apply the cipher sequence we get $C(E,c), C(E,c+1), C(E,c+2), \dots$

The key E is kept secret only the sender and receiver will know the key value. Here the sender would be sending the data with encrypting it with key E , and the data is sent via multiple nodes in wireless sensor networks. The node is selected using random permutation algorithm.

SSP is going to use this algorithm to protect it against selective jamming attack. After system initialization the WSN membership is static i.e., no sensor nodes will join or leave. First the SSP algorithm has to be executed at the end of every superframe. Every node executes the SSP algorithm permutation vector as an input data. As all nodes share the same permutation key and Secure Pseudo-Random Number Generator (SPRNG) in same state thus they compute the same permutation, thus the result is based on the SPRNG it is unpredictable for the hacker to know the permutation key. i.e., hacker couldn't recognize the slot.

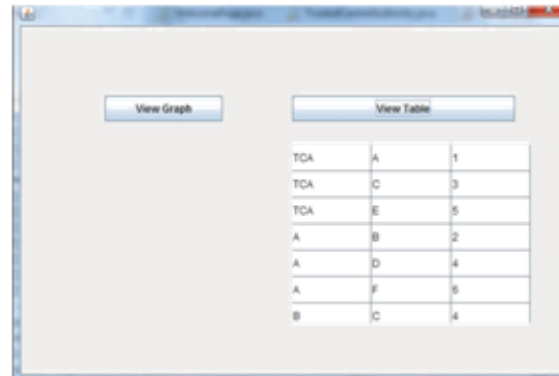
At any instant of time JAMMY allows the sensor nodes to join the network. By executing specific join procedure multiple nodes can be joined into the network. The join procedure assumes that every node has to perform the slot acquisition algorithm to gain a slot in the superframe for transmission of data.

VII. RESULT



Fig 9 directed graph

Figure 9 is a Directed graph, where the nodes which we are entered in node details of username are represented in this figure namely A, B, TCA, C, D, E, F. The link (Edges) between the nodes is entered in node details, which connect from one node to another node.



TCA	A	1
TCA	C	3
TCA	E	5
A	B	2
A	D	4
A	F	6
B	C	4

Fig 10 shortest route table

This figure10 shows the node details and BR value which gives shortest distance values between the nodes. By selecting the view table button 3 columns will be generated in the form of table first column will be the source node second column will be the destination node and third column represents the shortest distance between the 2 nodes. For example shown in figure consider A as the source node and B as the destination node here there will be many ways to reach from A to B but 2 will be shortest distance

VIII. CONCLUSION

JAMMI the dealt and effective solution to jamming attack in TDMA WSNs is proposed. This reduces the hacker to perform attack in random and reducing its effectiveness. It is difficult for the hacker to analyze the time and attack into the node. It introduces the no communication overhead nevertheless number of sensor nodes in the network.

IX. ACKNOWLEDGEMENT

The authors are thankful for the encouragement and support received throughout this work to Management, Principal of RRCE, Bangalore.

REFERENCES

1. "A Survey on Jamming Attacks and Countermeasures in WSNs" Aristides Mpitiopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou (2010). Denial -of-Service in Wireless Sensor Networks: Attacks and Defenses" David R. Raymond, Scott F. Midkiff (2011) . [3] "Jamming Sensor Networks: Attack and Defence Strategies" Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang, Rutgers University (2012).
2. Jamming-Resilient Multipath Routing" Hossen Mustafa, Xin Zhang.(2012).
3. Mitigation of Control Channel Jamming under Node Capture Attacks" Patrick Tague, Mingyan Li.(2013).
4. JAMMY: A Distributed and Dynamic Solution to Selective Jamming Attack in TDMA WSNs" Marco Tiloca, Domenico De Guglielmo, Gianluca Dini, Giuseppe Anastasi, and Sajal K. Das, Fellow, IEEE
5. Broadcasting the message over the network using different frequency and timing technique to bypass the jammers" Pooja.S, Pooja K.B (2017).