International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 2 Issue 6ǁ June. 2013 ǁ PP.41-46

An Effective Defensive Node against Jamming Attacks in Sensor Networks

P.Indumathi[1], P.Manikandan[2] and K.Yogitha[3]
[1][2]PG Scholar, Network Engineering and [3] Assistant Professor, ECE Department
Arunai Engineering College, Tiruvannamalai, India

ABSTRACT*-Resilience to electromagnetic jamming and its avoidances are difficult problem in wireless sensor networks .Jamming is one such Denial Of Service (DOS) attack that has been addressed at the physical layer and Energy Efficient Link Layer jamming attacks have proven to be a real threat to network communication for prolonged time.*

The intent of this paper proposes some changes in physical layer as well as Data Link layer. In Physical layer, uncorrelated groups based DSSS technique, which is a slender modification of DSSS used in sensor network standard, in which all possible 15 chip PN sequences are used to form groups of 5 sequences each and each group assigned an index and randomly selected.

In Data Link layer, SMAC (Sensor Medium Access Control) protocol contains two modifications. The first is Data Packet Separation Slot Size Randomization (DS-SSR); the second is Maximum Covers using Mixed Integer Programming (MC-MIP). DS-SSR is used to increase the WSN resistance against the Energy efficient denial of service link layer jamming attacks, MC-MIP is used to slightly eliminate the negative impact on the network throughput when using countermeasures against energy efficient jamming.

Lifetime advantage and censorship rate are the two measures used to evaluate the resistance of the proposed protocol against the attack. When compared to other counter measure experimental results shows more than 8% reduction of the attacker lifetime advantage can be achieved with DS-SSR and SMAC.

KEYWORDS*-DSSS; index; SMAC; jamming.*

I. INTRODUCTION

Wireless sensor networking is an emerging technology that has a wide range of potential applications including environment monitoring, smart spaces, medical systems and robotic exploration. Such a network normally consists of a large number of distributed nodes that organize themselves into a multi-hop wireless network. Each node has one or more sensors, embedded processors and low-power radios, and is normally battery operated. Typically, these nodes coordinate to perform a common task. Jamming is one such denial of service attack which prevents the network from performing its basic functions. Jamming is defined as interfering with the legitimate frequency of sensor nodes. Hence anti jamming techniques are essential in order to ensure timely delivery of information and to increase the performance of the network. There are various types of jamming such as sweep jamming, spot jamming, barrage jamming, deceptive jamming etc., [1] and many countermeasures are also proposed against jamming. Generally the countermeasures are classified into proactive techniques that are used to prevent jamming and reactive techniques that are used to overcome jamming. Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) etc., [2] are few proactive techniques and wormhole based anti jamming technique, hybrid model of defense etc., are few reactive anti jamming techniques. Energy efficient attacks target the Medium Access Control (MAC) protocol of WSNs. These attacks perform statistical analysis to select the proper time to jam in and sleep otherwise. An energy efficient jammer will not waste energy while preventing network communication for a long time compared to other jammer styles.

This paper is ordered as follows section II gives related works. Section III provides in detail about proposed modification to physical layer and SMAC protocol. Section IV provides the conclusion and suggestions for future work.

II. RELATED WORKS

In cagalj M et al (2005)[3] used Wormhole threat as a solution to bring out the message out of jammed area. This is done using three techniques namely (i) Wired pair of sensors, (ii) frequency hopping and (iii) uncorrelated channel hopping. In the first technique pair of sensor nodes is connected using wires and are deployed. The drawback of the technique is that it is complex and costly. In the second technique frequency hopping (FH) enabled nodes are deployed and then it is paired. The drawback of this technique is that it requires synchronization. In the third technique the sensor nodes opeirating on the same channel will be paired to transmit the measured even to outside the jammed area. This technique does not require any synchronization.

Mpitziopoulos A and Gavalas D (2008) [4] designed a prototype node named Ares that uses hybrid FHSS/DSSS to defend jamming attacks which is more efficient than existing techniques. Ares node uses a specific frequency hopping spread spectrum (FHSS) technique in 5 GHz band with 51frequency channels wherein the channel sequence is generated using a key which is derived from a secret word known only to the sensor nodes. Each channel uses direct sequence spread spectrum (DSSS) technique with 16 bit pseudo noise (PN) code. The Ares node can effectively defend the jamming attacks and also provides satisfactory packet delivery ratio. The drawback is that designing of the Ares node is complex. In [5] Mario Strasser et al. (2008) proposed an Uncoordinated Frequency Hopping (UFH) scheme which provides jamming free communication between two nodes in the presence of jammer without shared keys. UFH scheme is used for key establishment protocol that enables the nodes to agree on a shared key which will be further used to create secret hopping sequence and communicate using coordinated frequency hopping. It achieves same level of protection as frequency hopping technique. The drawback is that it has low throughput, high storage and processing cost.

Law Pajic and R.Mangharam[6] proposed the WisperNet communication protocol. This protocol uses the modules *(WisperNetTime), (WisperNetSpace)* to resist energy efficient link layer jamming.

i)*WisperNet-Time:*

This component in the WisperNet communication protocol is related to randomizing the timing properties of a TDMA protocol, this is accomplished by ***slot size randomization*** and ***schedule randomization*** **.**In ***slot size randomization*** nodes within the network are assigned a predefined key in nodes. In ***schedule randomization*** nodes change their transmission schedule randomly to further mislead the attacker however this may result in collision in transmission, which is resolved with preassgined node priorities.

ii)*WisperNet-Space:*

This module uses routing techniques to stay away from the jamming area, and it allows the nodes to moves away from the jammed area in a technique called *spatial retreat.*

III APPROACHES

A.UNCORRELATED GROUPS BASED DSSS TECHNIQUE

In this paper, an effective anti jamming technique is proposed to overcome the drawback of traditional DSSS technique. This scheme is a slight modification of traditional DSSS technique used in the IEEE 802.15.4 standard. Fig.1 shows the block diagram of the proposed scheme.

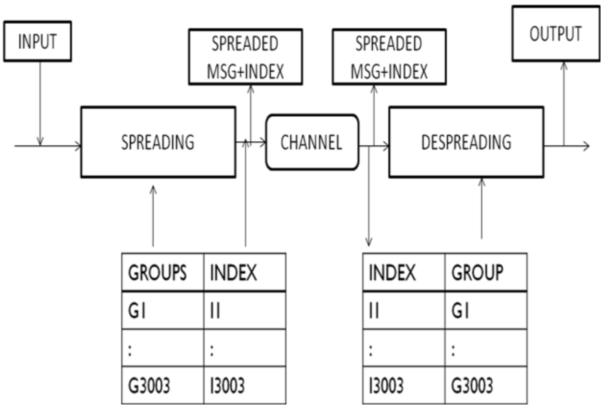

Fig 1Block diagram of uncorrelated groups based DSSS technique

This technique uses all possible sequences of 15 chip PN code to form groups with 5 sequences in each group. After forming these groups they will be permuted to form the group set. Each group in the group set will be assigned an index and these groups will be known to the sender and receiver. Totally 3003 groups are possible with the 15 chip PN sequence which is called as the group set. The measured event is spreaded with the groups that are selected for spreading from the group set. Each bit of the message is spreaded with different PN sequence present in the group. The index of the initial group selected for spreading is appended to the spreaded message and is transmitted through the channel. At the receiver side the groups are selected for despreading, starting with the initial group corresponding to the index which is received along with the received signal. The method for selecting groups for spreading is given in detail:

i) Formation of group set:

Let $\{Gi\}$ be the group set where$1 \leq i \leq 3003$, it is formed by permuting the possible combinations of 15 chip PN sequence. Each group in the group set will have 5 sequences, for example the group G_1 will have any 5 sequences from possible sequences given by $\{\ S_j\}$ where$1\leq j \leq 15$. Each group will be assigned an index denoted as I_k where$1\leq k \leq 3003$.

ii) ***Spreading process:***

The sender selects a group called as the initial group randomly from the available group set and its corresponding index is called as the initial index. In this technique each bit is spreaded with a PN sequence in the initial group and once the sequences present in this group are used, the next group will be selected such that it is totally uncorrelated with the initial group. The third group is selected such that it is totally uncorrelated with the previously selected group and so on. The groups are selected such that the successive groups are totally uncorrelated because if they are correlated it becomes easy for the jammer to decode more bits and hence capture the entire network. The groups that are selected for spreading should not be repeated. With this process 2980 groups are selected for spreading from the group set of 3003. After spreading the initial index is transmitted along with the spreaded message.

iii) ***Dispreading process:***

The receiver selects the group corresponding to the initial index, which is received along with the spread message as the initial group, for despreading. Once all the sequences are used in this group the next group will be selected such that it is totally uncorrelated with the previously selected group and it should not be repeated. These selected groups are used for despreading the received signal to obtain the original message.Fig.2 shows an example to transmit a message $m =\{\ m_l\}$ which has l bits, where$1 \leq l \leq 10$ For this two groups are required for spreading with 5 sequences in each group. Let G_{1823} be the initial group and its corresponding index is I_{1823} .

m_{10}	m_9	m_8	m_7	m_6	m_5	m_4	m_3	m_2	m_1
S_3	S_7	S_9	S_{10}	S_{14}	S_8	S_{11}	S_{12}	S_{13}	S_{15}
G_2					G_{1823}				

Totally uncorrelated

Fig 2 Example for the proposed scheme

This initial group is correlated with other groups present in the group set to find the totally uncorrelated group which is selected as the next group for spreading. Here the next group will be G_2 which has sequences totally different from the initial group hence they are said to be totally uncorrelated groups. Now the group G_2 is correlated with other groups in the group set excluding those which are previously used for spreading. Finally the groups used for spreading are {G1823, G2}. After spreading, the index I_{1823} is sent along with the spreaded message so that at the receiver side, the same algorithm is repeated to select the groups for dispreading starting with the initial group corresponding to the index $I_{1823.}$

The proposed technique is analyzed in terms of probability of groups matched and the traditional DSSS technique is analyzed in terms of probability of breaking the code. A wireless sensor network is simulated with hundred nodes in an area of 500x500 m2. As in IEEE 802.15.4 standard DSSS modulation is applied at all nodes. In traditional DSSS technique the nodes are assumed to use the same 15 chip PN sequence generated using N=4 shift register. For evaluating the performance of this technique, probability of breaking the code for the attacker is calculated in the presence of a single jammer and various numbers of jammer.

The probability of breaking the code is given by the number of successful trials to the total number of trials. Fig.4 shows the probability of breaking the code in the presence of jammers.

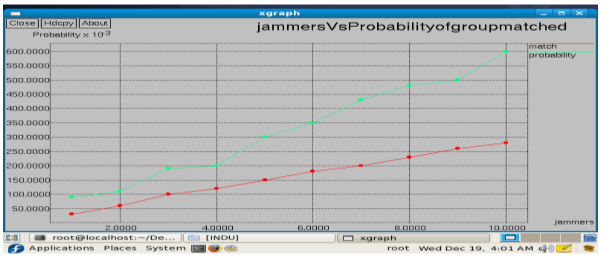

Fig 4-No of jammers vs. Probability of group matched

The probability has reached 0.6 in the presence of 10 jammers. It is inferred that as the numbers of jammer increases the probability can reach even 1 and once the code is broken the entire network can be captured. To overcome this drawback an effective technique is proposed. To evaluate the performance of the proposed technique probability of matching the groups is calculated in the presence of single jammer and various numbers of jammer. Here the probability of matching the groups is given by the groups matched to the total number of groups. Fig.5 shows number of trials vs probability of matching groups in the presence of single jammer.

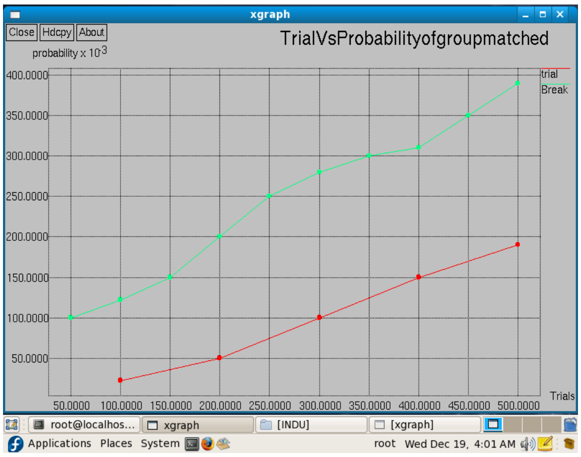

Fig 5 No of Trials vs Probability Of group matched.

With the previous notes taken into account, two modifications to the SMAC protocol are proposed to improve the resistance of SMAC protocol against energy efficient jamming while preserving the throughput of the network. The first is ***Data Packet Separation Slot Size Randomization*** (DS-SSR) to reduce the lifetime of the jammer. The second is ***Maximum Covers Mixed Integer Programming*** **(**MC-MIP).

IV. DATA PACKET SEPARATION

A typical statistical jammer follows a state diagram for the jamming process similar to Fig3 Observing interarrival times in the network is the basis of the jamming process. After observation, clustering is made to identify the slot size of the protocol used within the network.

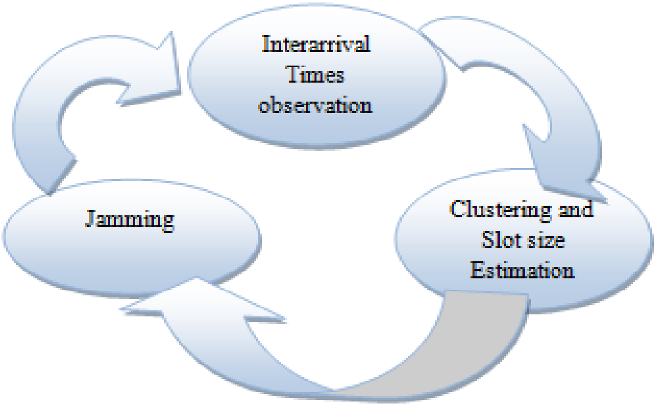
Interarrival Times observation
Clustering and Slot size Estimation
Jamming

Fig 3 Statistical Jammer cycle

If we manage to mislead the jammer to estimate the slot size smaller than it actually is we would succeed into forcing the jammer to jam at high frequency, we would make the jammer deplete its power source. When a legitimate node has data to send and the current slot is its allocated slot, the node sends in the control packet its desire to send data and the destination. The data part of the node is not necessarily large enough to fill the entire slot. We can separate the data packet into two or more parts. This works only for packets that are not too large that when separated the slot will not accommodate the separated parts. The separation process is not determined ahead of time and it is based on the size of the data packet to be transmitted so under certain situations, the node may separate data and in other cases, the node may not separate data. When the jammer observes the interarrival times of packets of the network, he gets the illusion of smaller interarrival time and hence a miscalculation of the slot size to be smaller hence jamming at higher rate this with have a dramatic effect on the lifetime advantage of the jammer.

The length of the jamming signal is time needed to transmit only one byte into the medium (the smallest size possible to transmit to preserve jammer energy as much as possible) .The power spend by an attacker PA is the sum of two components the first is power spend for the observation, clustering and slot size estimation Pc, which is a constant term not related to the rate of jamming, and the second component is the power needed to transmit jamming signals. The second component is based on the power needed to transmit a single jamming signal Pj, the estimated slot size μs, and the total jamming time t. the inverse of the estimated slot size μs represents the rate of jamming in a unit of time.

$$PA= Pc +t*Pj/ \mu s$$

Hence, the power consumed is inversely proportional with the estimated slot size. If for example a jammer miscalculated the slot size to be $\mu s' = \mu s /\alpha$ where $\alpha>1$. Let ΔP be the difference between the power spent by the jammer at an estimated slot size μs and the power spent at an estimated slot size μs’.

$$\Delta P= PA' - PA$$

$$\Delta P = Pc +t*Pj/ \mu s' - (Pc +t*Pj/ \mu s)$$

$$\Delta P = Pc +t* \alpha *Pj/ \mu s - (Pc +t*Pj/ \mu s)$$

$$\Delta P = (\alpha-1)*t*Pj/ \mu s$$

We note that ΔP is a considerable amount given and it increases as α increase. This would affect the lifetime advantage of the jammer, reducing the time that a jammer node can sustain an attack on the network.

When a node controls a time slot, it inspects the data that is about to be transmitted (if any) to decide if it can be further separated and what would the separation time. If the data packet is to be separated, the separation is specified in the separation Size attribute within control packet that is sent before transmitting the separated data packets. If separation Size is set to zero this means no data separation is about to happen.

V. MC-MIP ALGORITHM

```
Input: (T, D, M);
Output: A feasible schedule ΨLTF with minimal energy consumption;
sort all tasks in a non-increasing order of the computation requirements of tasks;
Xi ← φ and Xi ← 0 for i = 1 to M;
for i = 1 to |T| do
find the smallest Xm; (break ties arbitrarily)
Xm ← Xm + {τi} and Xm ← Xm + ci;
reorder Xi by a non-decreasing order of their loads and let XLTF ← {X1, X2, . . . , XM};
return the resulted schedule ΨLTF by applying MES (XLTF);
```

Let T,D, and$M$ denote the task set under discussions, its common deadline, and the number of cores, respectively. Algorithm LTF always assigns a task to the core with the smallest load, where tasks are picked up in a non-increasing order of their computation requirements. The seeking of the core with the smallest load could be done by the manipulation of a heap data structure. The time complexity of Algorithm LTF is $O\ (|T\ |\ (\log |T\ | + \log M) +M)$, which is dominated by the cost for task sorting and heap manipulation.

CONCLUSION

Energy efficient jamming is a real threat to WSNs as it assumes little knowledge about the network protocols and it can sustain an attack that is very effective, in terms of censorship rate and lifetime advantage, for relatively long periods due to its low power consumption and jamming attack that is effective against TDMA protocols such as SMAC, several countermeasures have been proposed to defend against this type of statistical jamming attack, and they tend to change the timing properties of the protocol used by changing the slot size randomly. In this paper, we present a novel countermeasure for TDMA protocols to defend against energy efficient link layer jamming attacks, this countermeasure targets the power consumed by the jammer, the main idea of the countermeasure is to separate the data packet into two parts. This separation results in misleading the jammer to estimate the slot size smaller than it actually is and to jam at higher rate hence, lose power faster. The defense is also equipped with a means to reduce slot size randomization effect on the throughput of the network by having all slots equal in duration by applying MC-MIP. Typically, slot size randomization results in a reduced network throughput due to randomized slot sizes among nodes resulting.

REFERENCES

[1]. Mpitziopoulos A; Gavalas D; Pantziou G; Konstantopoulos C; (2007)"*Defending Wireless Sensor Networks from Jamming Attacks*," Personal Indoor and Mobile Radio Communications. PIMRC 2007. IEEE 18th International Symposium on , vol., no., pp.1-5, 3-7

[2]. A.D.Wood and J.A.Stankovic, (2002) “*Denial of service in sensor networks*", Computer, 35(10), pp. 54-62.

[3]. CagaljM;CapkunS;HubauxJ.P; (2007)"*Wormhole-BaseAntijamming Techniques in Sensor Networks*," MobileComputing,IEEETransactions on, vol.6, no.1, pp.100-114.

[4]. Mpitziopoulos A, and Gavalas D, (2009) "*An effective defensive node against jamming attacks in sensor networks*"Security in WirelessSensor Networks,vol. 2,Issue 2, pp. 145–163.

[5]. M. Strasser, C. Poper, S. ˇCapkun, and M. ˇCagalj. "*Jamming-resistant key establishment using uncoordinated frequency hopping*". In Proceedings of the 2008 IEEE Symposium on Security and Privacy,pages 64–78, 2008.

[6]. M. Pajic, and R. Mangharam, "*Anti-jamming for embedded wireless networks*," in Proc. IPSN '09, 2009, p. 301-312.

[7]. (2011) The OMNET++ website. [Online]. Available: http://www.omnetpp.org

[8]. Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "*Wireless sensor network survey*," The International Journal of Computer and Telecommunications Networking, vol. 52, pp. 2292–2330, Aug. 2008

[9]. Ruizhong Lin, Zhi Wang, and Youxian Sun, "*Energy Efficient Medium Access Control Protocols for Wireless Sensor Networks and ItsState-of-Art*," IEEE International Symposium on Industrial Electronics, vol. 1, pp. 669 - 674, May. 2004.