Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 1– No.2, January 2015 – www.caeaccess.org

A Novel Approach to Hinder Jamming Attack in WSN

Annu Joshi
Research Scholar
Banasthali Vidyapith
Tonk Distt, Rajasthan

G.N.Purohit
Dean of Apaji Institute
Banasthali Vidyapith
Tonk Distt,Rajasthan

ABSTRACT
Wireless sensor networks (WSN) are used in many scientific and technological fields. They are used in many mission critical events nowadays in which the information/message availability, authentication and integrity is most important phenomena for the rescue operation. It is imperative that WSN should be immune to jamming attack which is a form of denial of service attack in WSN.In navigation system where information is to be spread among several motes (approximated among untrusted receivers), availability of precise information is a must. Similar is the situation in emergency alert systems. General available techniques such as frequency hopping and direct sequence techniques cannot be applied in such scenario because these depend upon secret pair wise key which is shared between the sender and the receiver before communication. This dependency has adverse effect on network because it makes the system un-scalable as well as more attack prone, e.g. when a single mote is compromised by attacker whole system is hijacked by the attacker. In this paper, we introduce un -coordinated spread spectrum techniques which do not share secret key before communication.Un coordinated spread spectrum technique can handle the unlimited numbers (most of them malicious) of receivers. Using USS techniques, the message size increases and in this way slow down the transfer speed of the message. To overcome this demerit of USS, a novel approach is presented in the paper by combining the uncoordinated spread spectrum (USS) technique with mobile agent techniques. This scheme overcomes the shortcomings of USS.

Keywords
WSN, Spread spectrum, Frequency hoping, Direct Sequence Spread Spectrum, Mobile Agent, Cryptography.

1. INTRODUCTION
The market of WSN is growing very fast.. In the late 1990s, it became clear that Moore's Law will eventually boost performance of WSN and bring down power consumption. A sensor node is low cost, small sizes and comprehensive power option .These are used in many mission critical operations such as navigation system, emergency alert system, health monitoring (heart rate, glucose monitoring and cancer detection),in industries, traffic management and smart home, etc .These sensors are currently also employed for detecting deterioration in bridges, flyovers etc(U.S. is using sensor detectors for bridge overlooking). According to a study by Venture Development Corporation, the worldwide market for wireless measurement devices and services provided by WSN is expected to reach over $US 1.5 billion by 20121.There is very promising future of sensors in the next 10-15 years. A survey done, on market strength of WSN ,in 2007 for estimating its future proportion in the market is shown in Figure 1.

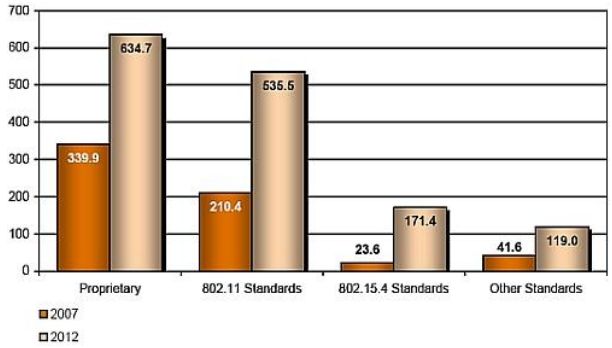

Figure 1: Growth estimation in WSN

Wireless sensor networking protocols have matured to overcome the challenges associated with earlier technology. Owing to its wide spread uses in daily life and in some mission critical events, it has to be strictly secured to jamming attacks. Spread Spectrum (SS) techniques represent a common way to achieve anti-jamming in communication systems. These SS schemes share pair-wise secret keys before communication. Important spread spectrum techniques are Frequency Hopping (FH) and Direct-Sequence Spread Spectrum (DSSS). Essential for both FH- and DSSS-based communication is that the sender and the receiver share a secret key prior to communication, which enables the receiver to generate the random sequence and to detect and decode the sender's spread signal. This reliance on a pre-shared secret key generally precludes unanticipated transmissions between unpaired devices as well as communication from a sender (or base station) to an unknown set of receivers (some of which might be malicious and try to compromise the messages of other receivers). This problem can best be illustrated as follows: If a base station wants to broadcast a message to a set of receivers in a jamming-resistant manner, it would need to share one or several secret spreading sequences with all the receivers, and the sequences would need to be hidden from the attacker (that could otherwise jam the transmissions using the spreading sequences). In a number of scenarios—such as in those where receivers cannot be trusted or where they are unknown before the actual communication (e.g., in local or global navigation systems).The assumption for shared secret spreading sequences is unrealistic and will typically prevent the application of anti jamming communication. This problem is termed as the anti-jamming broadcast problem. Out-of-band key pre-distribution between the sending and receiving devices generally does not solve the anti-jamming broadcast problem: key pre-distribution is not feasible in the case of unknown receivers (e.g., for navigation) and even if the receivers are known, it suffers from serious scalability issues. An established public-key infrastructure does not solve this problem either because SS techniques require shared secret keys and the devices still need to communicate in order to agree on a shared secret (Diffie-Hellman) key while

communicating may be impossible in the presence of a jammer. This leads to an anti-jamming/key-establishment dependency cycle. In this paper, we introduced a technique which is a combination of two techniques, i.e. spread spectrum technique and mobile agent technique which compensate the drawbacks of each other and making the network model more dynamic and jamming free. In this paper, section 2 is about the previous work done in jamming in WSN.Section 3 talks about the problem description. Section 4 and 5 is about proposed model of WSN and implementation details respectively. Section 6 is about the simulation result of the proposed technique. Finally section 7 is about the conclusion and future perspective of this work.

2. PAGE SIZE

Wireless communication jammers have been widely analyzed and categorized in terms of their capabilities (e.g., broadband or narrowband) and behavior (e.g., constant, random, responsive, sweep) [1], [2], [3]. Many jammer models used in prior works [1], [2]–[4] cover the interference with transmissions in terms of signal jamming as well as dummy packet/preamble insertions. In [5], [6], the respective authors address broadcast jamming mitigation based on spread-spectrum (SS) communication. Common to these broadcast schemes as well as to other proposed countermeasures against denial-of-service attacks in wireless networks [2], [4], [5]–[7] is that they all rely on secret keys, shared between the sender and receiver(s) prior to their communication. However, pre-establishing keys between devices in ad-hoc networks for subsequent SS communication suffers from scalability and network dynamics problems. Key-establishment approaches that rely on device proximity [8]–[12] can be used in this context, but require the nodes to be physically close to each other and to use communication channels that are not being jammed (e.g., infrared, wire, or visual). Furthermore, if some of the receivers in multi- or broadcast communications are not trustworthy, relying on preshared or established group keys allows malicious receivers to receive messages themselves while withholding (jamming)or modifying them for others [20]. Unlike these approaches, the proposed USS schemes enable (broadcast) communication anti-jamming and key establishment over longer ranges using exclusively radio communication channels. Recent observations [13], [14] identify the shortcoming of non-existing methods for jamming-resistant communication without shared secrets and propose solutions to this problem [13]–[15]. The solution proposed by Baird et al. [13] uses concurrent codes in combination with UWB pulse transmissions. The achieved jamming resistance is, however, not one-to-one comparable to spread-spectrum-based techniques: While the attacker of SS techniques must have enough transmission power to overcome the processing gain, in [13] the limiting factor is the number of pulses that the attacker can insert, i.e., the energy of the attacker. Jin et al. [15] propose zero pre-shared key DSSS to establish a secret key between a pair of nodes; in contrast to our USS schemes, their solution is targeted for pair wise communication. Dolev et al. present f- AME [14], a round-based, randomized protocol to set up group keys in the presence of message collisions and insertions, but require a (fully connected) group of size > 3(t+1)^2 +2(t+1), where t is the number of channels that the attacker can jam (usually t is in the order of tens or hundreds of channels requiring a group of hundreds or even thousands of nodes). In addition to [14], a substantial number of theoretical and algorithmic results on jamming-resistant networking have been achieved recently, examples include [16]–[19]. The proposals address multiplayer problems under malicious interference, such as anti-jamming MAC protocols [16], gossiping [17], neighbor discovery [18], and leader election and binary consensus [19]. In this paper, we propose Uncoordinated Spread Spectrum (USS) techniques that enable anti-jamming communication between sender and receivers that do not share any secret keys. These techniques constitute a solution to the problem of anti-jamming broadcast and anti-jamming key establishment. USS techniques randomize the selection of the spreading key (sequence) such that neither external attackers nor malicious (dishonest) receivers (insiders) are able to jam the communication in a targeted way (the best they can do is to jam using guessed spreading sequences similar to jamming coordinated SS techniques); legitimate USSS receivers only possess public information that cannot be misused for targeted jamming. The jamming resistance of USS communication is comparable to the jamming resistance of their coordinated counterparts. USS techniques achieve this by removing the requirement of pre-shared secrets (keys) at the expense of a reduced communication throughput. On the other hand, there is a concept of mobile agent technique, in which a program or software can track the attackers on the way. Our contributions in this paper are that we are proposing a novel approach which is a combination of two powerful techniques, combination of spread spectrum technique with mobile agents.

3. PROBLEM DESCRIPTION

There are three types of anti jamming strategies

i Proactive techniques: These are active in background even if in the Jamming free environment, such as DEEJAM algorithm. These techniques are costly and energy consuming techniques, such as DEEJAM algorithm.

ii Reactive Techniques: These techniques are active only in jamming attack sensed by the network,e.g. JAM algorithm.

iii Mobile agent techniques: In this system, mobile agents (MA) are used.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,e.g. ANT system and JAID algorithm. No extra hardware cost is required but drawback is that no expanded simulation is done. The drawback of JAID algorithm is that it cannot defend the WSN in case the jammers exercise efficient attack against all nodes simultaneously.

Besides them spread spectrum techniques can be used for anti jamming in WSN. These are of two types:

i Frequency hopping: it is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels using a shared algorithm known both to the transmitter and receiver.

ii Direct sequence: It is performed by multiplying the data with a pseudo noise digital signal. The advantage of these techniques is that reduction of interference and attacker cannot decode the pseudo code easily and this provides security.

But in spread spectrum technique, there is a limitation that the transmitter and receiver should share a secret key and on

behalf of that they can exchange information but in a scenario where some receivers cannot be trusted or where they are not known in advance, the assumption about shared secret key code is unrealistic and will prevent the application of anti jamming communication. In the situation when an alert is disseminated to the public and there is jamming in some area if shared secret key is disclosed then it would create the problem to disseminate the alert., To resolve this, uncoordinated SS techniques can handle large amount of malicious motes., USS techniques are beneficial to the network since it works in the dynamic manner but there are some drawbacks which are associated with it:

i More connections lowers the possibility of error free messages.

ii Large format of messages for security purpose which further enlarge the message, so fast communication is affected.

These drawbacks can be compensated by introducing MA techniques which are autonomous programs along with the USS technique. So, whatever connections we have, there are less chance of error prone messages and also efficient tracking of whole system.

Further mobile agent techniques do not require hardware. So, in addition of spread spectrum techniques, these mobile agents can enhance the techniques.

4. PROPOSED MODEL

In our hypothetical model, we presume that there is a sender S and its all around a set of receivers {R1;R2……Rn} which are in transmission range of sender S.We also presume that the each node is capable of sending radio transmission which also enables them to receive the signals. This can be done by virtue of Spread spectrum technique. We will consider only frequency hop spread spectrum technique, which involves communication according to desired frequency channel and use the concept of un-coordinated FHSS technique. For the security purpose, sender would send same frequency channel for a short span. The message which has to be sent is thus split into a set of fragments with a unique size (approx. a few hundred).The sender sends each fragmented packet after encapsulation of each packet with the error encoding code and send it in random manner so that adversary could not jam the message. Further this model is also based on assumption that adversary cannot jam all the network simultaneously and sensors mobility is not considered here. This is all about the hard-ware setup for proposed model. In addition to this, we also traverse the network with a mobile agent programme which simultaneously track the network to identify jammed region. The mobile agent is assumed to be tamper resistant and has a timer which is synchronized with the base station. By virtue of UFHSS, sender randomly selects the frequency channel among the set of frequency band available. To receive the signal, the receiver needs to be synchronous to the frequency send by sender. The message is sent in a fragmented manner and encoded. The receiver assembles the message and decodes the same. Public key cryptography in (ECC) is used in this technique. Since the sender openly sends its signal frequency in all the direction, so an adversary at that time can detect the frequency mode desired and can attack the message or node. But the adversary can't interfere the broadcast of the message to other nodes. On the other side, mobile agents detect the jammed region and they can inform the base station. In this way, sender can re-route its sending path. So, the scared and costly bandwidth of the network is efficiently managed by its. MA trackers constantly connected to base station and informing us about the adversary. In UFHSS technique without MA, we have to use large no. of cryptographic keys, which in turn make the communication of large messages cumbersome and much delayed as compared to small size messages. Now, with MA, filtering of adversary is occurring, so no need to use large length of cryptographic keys. The robustness of the network depends upon the predicted MA's energies and the distance between the nodes. The distance between the source node and the destination nodeis given by the distance formula.

$$Dij = [((Xi - Xj)^2) - (Yi - Yj)^2$$

Here, (Xi, Here, (Xi,Xj) is the Cartesian coordinates and I is the source node and the j is the destination node. Wireless node takes more energy then wired networks, so, distance between the nodes is squared; energy dissipated by the node is thus

$$\Delta Eij = \frac{L}{(Dij)^2}$$

Here L is the present link budget available to the node. The agents avoid visiting nodes with depleted energy by determining alternative routes in the sensor network. Thus the network remains partially functional even if some of the individual sensors fail.

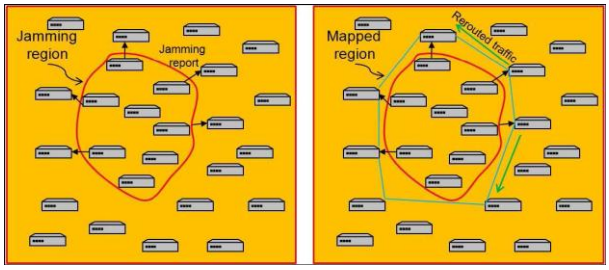

Figure 2: Jamming alert in routed traffic by Mobile agents

5. IMPLEMENTATION DETAIL

In order to demonstrate the feasibility of the proposed uncoordinated spread spectrum communication techniques, we created a prototype implementation based on Universal Software Radio Peripherals (USRPs) [13] and Gnu Radio. The USRPs include an A/D (D/A) converter that provides an input (output) sampling rate of 64 Mb/s (128 Mb/s) and an input (output) sample resolution of 12 bits (14 bits); the employed RFX2400 daughterboard are able to use a carrier frequency of 2:3 □ 2:9 GHz. In this setup, the USRPs were each connected via a 480 Mb/s USB 2.0 link to a Lenovo T61 ThinkPad (Intel Core 2 Duo CPU @ 2.20 GHz) running Linux (kernel 2.6.27) and Gnu Radio (version 3.0.3). For performance reasons and for ease of deployment, our sender and receiver applications were written entirely in C++, which required porting some Gnu Radio libraries from Python to C++. Moreover, to achieve synchronization between writing the signal data to the USRP and the actual signal generation that is accurate enough to enable frequency hopping, the USRP drivers had to be adapted. Further autonomous program is to be installed in USRP so that tracking can be done in systematically.

6. SIMULATION RESULT

We have examined a variety of scenarios taking into account various aspects (e.g., jammer and nodes antenna gain, path loss, etc.).The topology of jammer and nodes/sink is random and is used throughout all our simulation tests. A sensor network with 16 nodes is considered in this simulation run with agents randomly placed on the nodes. After converging, the mobile agents adapt to the network using the knowledge acquired from their neighbors The proposed detection and defense mechanism is simulated using Matlab R2007a. The performance of the network is evaluated on basis of varied Jamming to signal ratio (J/S), energy to jamming density ratio, energy to noise density ratio, multi-path interference, the number of agents employed in the network is 16. The stability of the mechanism is analyzed by iterating all scenarios for 100 runs. The actual hops are user defined which varies depending on the problem assigned.The predicted energy and distance helps in making a decision whether the nodes in the current route are still capable of communicating with its peers in the next iteration. Table 1 show the performance of the sensor network, when a single tone jammer is applied. Initially, the number of jammed node in a period t seconds is 4. Hence, the number of nodes jammed is 4 out of 16 in the network. Similarly in each case nodes are jammed for t seconds. Since single tone jammer affects only one carrier, and the modulation used here is UDS/UFH, therefore the probability of interfering the alert message is low by the adversary.

In the case jammer attacks in a specified frequency domain, the corresponding results are given in Table:

Table 1

Node jammed	Average distance	Average energy	Average packet loss	Average packet delivery
4	10.205	17.345	0.030	98.009
8	27.051	25.987	0.085	96.789
12	38.078	32.234	0.316	85.678
16	97.765	52.145	0.397	83.006

In the case a jammer attacks in multiple frequency domain, the corresponding results are given in table

Table 2

Node jammed	Average distance	Average energy	Average packet loss	Average packet delivery
4	5.007	2.897	0.010	100
8	5.786	5.456	0.020	95.776
12	19.007	40.563	0.100	87.569
16	92.675	90.675	0.200	76.009

7. CONCLUSION AND FUTURE WORK

There are amazing benefits of using un coordinated spread spectrum techniques.USS provides dynamic architecture to WSN and it is a must for mission critical events. We propose a novel approach to combine MA technique to spread spectrum techniques, so that utilization of these two techniques can be achieved.USS techniques can be optimized by mobile agent techniques. A more general direction for future work consists in exploring the impact of jamming, not only on the physical layer but on all layers of the network stack. Above all, one needs a better understanding of (distributed) jamming attacks that target particular, application-specific traffic characteristics and exploit the distributed nature of most applications. Future work is also planned to get more insight into what kind of attacks are feasible on the physical layer, under which conditions, and at which costs, in order to improve existing attacker and jammer models.

8. REFERENCES

[1] R. A. Poisel, Modern Communications Jamming Principles and Techniques.Artech House Publishers, 2006.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launchingand detecting jamming attacks in wireless networks," in Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking andComputing (MobiHoc), 2005.

[3] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in Proceedings of the IEEE International Conference on Computer Communications(Infocom), 2007.

[4] M. C˘ agalj, S. C˘ apkun, and J.-P. Hubaux, "Wormhole-based antijamming techniques in sensor networks," IEEE Transactions on Mobile Computing, vol. 6, no. 1, pp. 100–114, 2007

[5] J. Chiang and Y.-C. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in Proceedings of the IEEE International Conference on Computer Communications (Infocom), 2008.

[6] Y. Desmedt, R. Safavi-Naini, H. Wang, C. Charnes, and J. Pieprzyk, "Broadcast anti-jamming systems," in Proceedings of the IEEE International Conference on Networks (ICON), p. 349, 1999.

[7] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," SIGMOBILE Mobile Computing and Communications Review, vol. 7, no. 3, pp. 29–30, 2003.

[8] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in Proceedings of the 7th International Workshop on Security Protocols, Springer-Verlag, 2000.

[9] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in Proceedings of the IEEE Symposium on Security and Privacy, 2005.

[10] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, "Loud and clear: Human-verifiable authentication based on audio," in Proceedings of the IEEE International Conference on Distributed Computing Systems, 2006.

[11] S. C˘ apkun and M. C˘ agalj, "Integrity regions: authentication through presence in wireless networks," in Proceedings of the 5th ACM workshop on Wireless Security (WiSe), 2006

[12] C. Gehrmann, C. J. Mitchell, and K. Nyberg, "Manual authentication for wireless devices," RSA Cryptobytes, vol. 7, no. 1, 2004

[13] L. C. Baird, W. L. Bahn, M. D. Collins, M. C. Carlisle, and S. C. Butler, "Keyless jam resistance," in Proceedings of the IEEE Information Assurance and Security Workshop (IAW), pp. 143–150, June 2007.

[14] S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport, "Secure communication over radio channels," in Proceedings of the 27th ACM symposium on Principles of Distributed Computing (PODC), 2008.

[15] T. Jin, G. Noubir, and B. Thapa, "Zero pre-shared secret key establishment in the presence of jammers," in Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 219–228, ACM Press, 2009.

[16] B. Awerbuch, A. Richa, and C. Scheideler, "A jamming-resistant MAC protocol for single-hop wireless networks," in Proceedings of the ACM symposium on Principles of Distributed Computing (PODC), 2008.

[17] S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport, "Gossiping in a multi-channel radio network (an oblivious approach to coping with malicious interference)," in Proceedings of the 21st International Symposium on Distributed Computing (DISC), pp. 208–222, 2007.

[18] D. Meier, Y. A. Pignolet, S. Schmid, and R. Wattenhofer, "Speed dating despite jammers," in Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), 2009.

[19] S. Gilbert, R. Guerraoui, and C. Newport, "Of Malicious Motes and Suspicious Sensors," Theoretical Computer Science, vol. 410, no. 6-7,pp. 546–569, 2009.

[20] M. Kuhn, "An asymmetric security mechanism for navigation signals,"in Proceedings of the Information Hiding Workshop, 2004.