International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 8 (2015) pp. 20489-20498

http://www.ripublication.com

Real Time Implementation of NCFHS Algorithm In Wireless Sensor Network For High Data Security

Muruganandam. A[1], Dr. Anitha. R[2]
[1]*Research Scholar, Bharathiar University,*
Coimbatore, Tamilnadu, India.
murugan.andam@yahoo.co.in
[2]*Research Supervisor, Muthayammal Engineering College,*
Bharathiar University,Coimbatore, Tamilnadu, India.
aniraniraj@rediffmail.com

Abstract

Secure data transmission in WSN is an important factor to be achieved. Method of implementing data aggregation, slicing and cryptography might safe the transmission, but adds complexity to the network. Our novel method is designed to achieve high data security by Neighbor-Count Based Frequency Hopping Secured Routing (NCFHS). NCFHS has implemented both hardware and simulation and the results have been studied. From the results obtained through a number of experiments our novel approach NCFHS has been found as efficient in securing data transmission.

Keywords: adhoc, frequency hopping, spread spectrum, security , wsn.

Introduction

The easy deployment of wireless sensor network replaces wired and other wireless networks. The formation of WSN is simple and affordable and does not depend on any centralized route or base station. All intermediate nodes would carry and forward the packets and should act as routers. Moreover, the transmission sending node may, on initialization of packet, need flooding its packet entirely to its neighbor. These factors would introduce more points of vulnerability. Thereby threat to has become an important feature in WSN.

Several approaches to the subject have been proposed in recent times. However, results of good effort in terms of security have not been seen. Data aggregation methods may eliminate unwanted flooding, but intruder attack on that particular data aggregated node would unveil more data collected about the network. Interruption, Interception, modification and fabrication are the major elements which affect security of the network. Interruption leads to loss in packet transmission, during

which more nodes try to access a single node. A single node receives data from a large number of neighbors. In interception, an unauthorized node would get access and trap the information shared among the network. Attack by modification is used to change the content of the original data. In fabrication, adversary nodes flood wrong information like false routing table in the network.

Integrity of packets that ensure no modification of the original information and confidentiality related to the factor that the node involved in conversation is an authorized one and being the major criterion to be ensured in WSN.

The earlier methods suggested addition of more checksum information along with the original data that introduce complexity in the network. In this paper, we propose the use of a neighbor count based frequency hop selection algorithm which can keep network away from these security threat.

Related Works

Packet hiding is one of the methods used for secure packet transmission. In this method, packets are sent with some cluster of overhead packets. At the receiving end using some encryption the cluster data is removed and the information is decoded. The drawback of this method lies in the consumption of more power than seen in normal packet transmission. Hence the lifetime is reduced [1]. In selective jamming attack, an adverse node is used to get maximum utilization. This results in the inability of other nodes could not utilize it. Hence the network gets hanged. It could be found by end to end delay function and energy consumption. But it will not be accurate because normally the end to end delay and the energy consumption varies with the distance between the two nodes [2].

In the slicing and resembling method, Data aggregation slices packets into multiple smaller packets and sends them to the neighboring nodes. Each node receives the smaller packets, reconstructs packets and reverts back to the data aggregation node. The data aggregator resembles any received packet and retrieves the original data. The main issue in this method is that even a movement of a single node away from its position would cause the loss in the portion of the packets [3].

Frequency hopping has been recommended in some methods in which all contributing nodes follow a common procedure or rules for hopping. On compensation of single node, an entire network could be hacked by an intruder. Nodes share similar keys for every transaction. They are not fair for secure communication.

The WSN plays a very important role on indoor and outdoor unit the network life time is based on timeliness and correctness of data [5]. multiple number of vulnerabilities tack to counting a every attack in the method.

In wireless sensor network data accumulation is difficult [6] use of the homomorphism technique increases the security as data encryption is done with different keys, which are secure within the hop to hop but not end to end.

Wireless communication is very sensitive to radio interference [7]. In this mechanism, the failed packet is first detested using a low-rate overlay link layer. This reduces packet jamming and overcomes security problems.

The Multi hop wireless networks help to increase the reliability compared to the single hop networks [8], using orthogonal channels. They use a gate way for providing high security. So this method is used to increase the number of channels.

In paper [9] interference based channel selection is proposed. Here, routers are initially availed with a set of channels and basic capacity. Number of radio channels and afforded data rate to each channel and it relies on congestion and throughput and loss ratio. The channel interference is caused by many factors, including a one hop distance.

Slotted seeded channel hopping [10] traffic has been randomly distributed to all nodes and partial synchronization with source and destination has been discussed. Its demerits are identified as non-synchronization between nodes which further reduce the data rate of transmission. Quorum-based framework [11] eliminates the bottle neck problem seen in a single control channel. Dynamic spectrum access by global control channel would be a factor eliminated by inducing two quorum channels where on initialization of network all nodes identified to work at these quorum channels through which the uniform distribution of rendezvous points and the minimization of time taken between two channel hopping has accomplished.

Adhoc -probe [12] is method in which bottle neck link capacity has been found earlier by applying two back to back packets-Both were separated by time duration related to bottle neck. Since the time duration induced between two hops is not the same and factors of distance and transmit powers, increase the unsuitability of Adhoc-probe.

In [13] static channel assignment has been recommended based on a few metrics such as end to end metric, cardinality and maximum of minimum transmit power has measured and based on which the static channel has assigned. All clusters are assigned their own edge limits. The formulated edges chooses new static channel which has a value beyond certain interference.

[14] Polytope code is used for security purposes. It splits the packets in to a number of smaller packets and best utilization of all nodes has been achieved through this process. The anomaly node has been found by applying polytope codes and found suitable for larger scale network rather than small scale network.

Methodology

A.Selection of Channel

Any communication link requires synchronization between nodes and users which cannot be achieved when a mismatch happens. This may results in the dropping of packet transmission.The formulated edge chooses new static channel which has a value beyond certain interference. Based on these fundamental concepts, any intruder could pickup data on air by setting the similar frequencies. Data hiding and encryption method has been proposed earlier. For avoiding this issue this encryption and data hiding method modifies the original content of the data and adds headers to the original packet. It causes increase in overheads and additional traffic to the network. Encryption and decryption would be time and memory consuming processes for all

contributing nodes involved in communication. Key sharing between notes is still a challenging problem despite offering security in data. This paper proposes the neighbor count based frequency hop selection. In this method, each node of network calculates its own hopping sequence based on the neighbors of two communicating nodes. All nodes use a certain bandwidth of spectrum for resources. Multiple channels accompany within a particular bandwidth. There should be a sufficient guard band or band gap between successive channels in available bandwidth. Number of frequency hopping ensures greater security to the network. On initial negotiation between two nodes it shares the knowledge about their number of neighbors. Based on count of its neighboring nodes and these variation, these two nodes are asked to hop to new frequency and continue transmission. Whenever this number in neighbor count varies, the hopping also varies for both nodes involved in conversation. This switching between available channels has to synchronize for launching proper communication. In the case of slow hopping, the number of changeover might consume less power, but network might be vulnerable to security threat. In a pool of available bandwidth resources, if larger number of channels are available, then this paper highly recommends fast hopping. All nodes are assumed to have knowledge of common algorithms used to select the new hop.

B. Hop Selection Algorithm

In hop selection based on neighbor count, each node calculates some set of frequencies. In each set consists of set of channels.

Fs1 = {F1, F2, F3, F4}

Fs2 = {F5, F6, F7, F8}

Calculated frequency in the first set of frequency would be an output for preparing a second. In case any node senses its count on neighbor varies correspondingly i.e. rather on depends on past set calculated, it forms a new set as per the neighbor count. It is not necessary that both communicating nodes should have the same number, of neighbors. So those nodes need to communicate with are another requiring sharing information on the neighbor count.

Fh1 = nbr(sr) * [nbr(dst) + nbr(sr) * nbr(dst) + nbr(sr) * nbr(dst)] / (2.048 * nbr(src) + nbr(dst) * pow(10,6)]

From frequency Fh1, others including F1, F2, F3, F4 would be derived. Similarly, F5, F6, F7, F8 would be predicted from earlier sets. Among a multiple set of frequencies, the earlier set be the input to predict the consequences of sets, if the network does not differ in neighbor count. In case, any of involved node senses a new neighbor or existing neighbor moves away its counterpart has to be informed regarding the changes. Again it has to find a new set of frequencies and hence both nodes must follow a new hopping sequence to have synchronization with each other.

Algorithm

1. Node needs to communicate, initiate request to particular node by sending an request indicates neighbor count. *Nbr*src,
2. Destination node responds to request made by src by sending *Nbr*dst. Both *Nbr*src and *Nbr*dst noted by all intermediate node.
3. All nodes start to calculate the primary hop sequence and its consequences set Fs1, Fs2.
4. Sequentially communicate with each other by regular hopping.
5. Check for changes in *Nbr*src and *Nbr*dst . If any changes identified follow from step i in routine.
6. Or else continue from step iv.

C. Hardware Implementation

On implementation of this neighbor count based frequency hop selection; MC1321x Freescale ARM processor is used. The figure 1.1 shows the photograph of the Hardware implementation setup.It has 2.5GHz bandwidth. In the available bandwidth this MC1321x has 16 channels. In bandwidth resources, IEEE 802.15.4 has 16 channels with in 2.4 GHz band, It ranges from 2.405 GHz to 2.4835GHz. This fr Each node is equipped with one micro controller PIC16F877a, one wireless transceiver antenna, 12v battery. All nodes are used for sending data serially between them. For these Max232 is used for level converter between RS232 and TTL logics. Attention (AT) commands sent serially to Freescale module for its configuration. Freescale ARM processor operates at command mode and data mode, in which a command mode used for its configuration where it decides about the destiny node. In data mode, the packet which needs to be transmitted will be sent. Both modes of free scalar has are controlled by the attached controllers.

Figure 1.1: WSN Hardware Setup

Here the controller has emulated with our proposed algorithm and takes decision on channel hopping as per our algorithm. PIC 16F877a is used. It has some memory for carry and forward architecture. Each PIC 16F consists of data RAM 368 x 8 bytes and EEPROM up to 256 x 8 bytes. Here frequency hopping is calculated based only on the adjacency detail of source and destination. If there is any intermediate node

existing between source and destination, all nodes contributing in communication are informed about the change in network. Serial communication exists between the master controller and MC1321x and between two nodes. Packets in controller received serially are converted to parallel and the entire packet is subjected checked against specified algorithm. All received packets are viewed and the controller identifies about source and exact destiny and its neighbor count and performs hoping. Otherwise each inlet packets are subjected to rules as specified in the proposed algorithm and selects a new channel. Demerits of data aggregation and encryption have been eliminated in this paper.

Results and Discussion

A.Simulation Parameters

A Network Simulator Ns-2.35 has been used for simulation. In which a code for proposed algorithm has been written in Tool Command Language. In the specified algorithm the neighbor of each node has been found upon execution of Tcl file. Neighbor list is the major input to the algorithm. The node like model has been viewed in network animator Nam 1.15. Totally 12 no of nodes deployed in network. Each is configured to have a 500 meter transmission coverage in simulation. Similarly all participating nodes are configured to have an Omni antenna, which covers 360 degree. Each node floods requests to the neighboring nodes and the nodes responds with reply. Based on the number of replies from the nodes, each node decides number of count its and shares these values with the node to one which needs to communicate.

Table 1.1: Simulation Parameters

Number of nodes	12
Area Size	700 x 700
Mobility model	Random Way Point
Traffic's type	CBR
Channel capacity	2 Mbps
Transmit Power	0.3 J
Receive Power	0.3 J
Sense Power	0.02 J
Idle Power	0.01 J
Initial energy	50 J
Communication system	MAC IEEE 802.15.4g

All nodes deployed at simulator are configured as mentioned in Table 1.1. By varying the traffic size respective packet delivery ratio also varies. It is plotted in Fig 1.2.

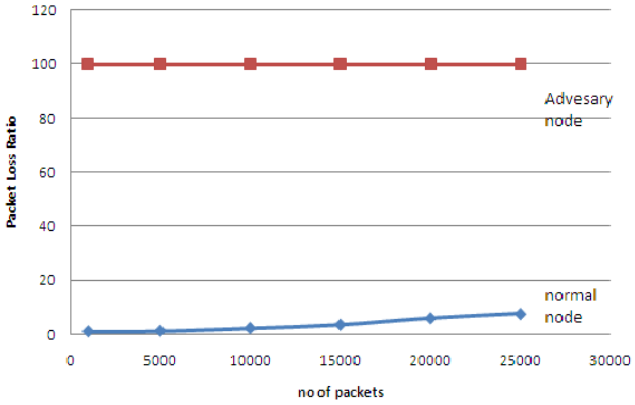

Figure 1.2: Packet Delivery Ratios

Variation of the number of packets sent from the source node helps measurement of the number successfully received at destination. The ratio between numbers of packets sent and received is the packet delivery ratio. Here adversary node does not have knowledge about the neighbor count based hopping. When an intruder or attacker tries to flood its packet to the network, it would not be picked or received by any nodes and hence most of transmitted packets from intruder suffers heavy loss. So packet delivery ratio is poor than nodes and is synchronized. This is shown in Fig 1.2 and Fig 1.3.

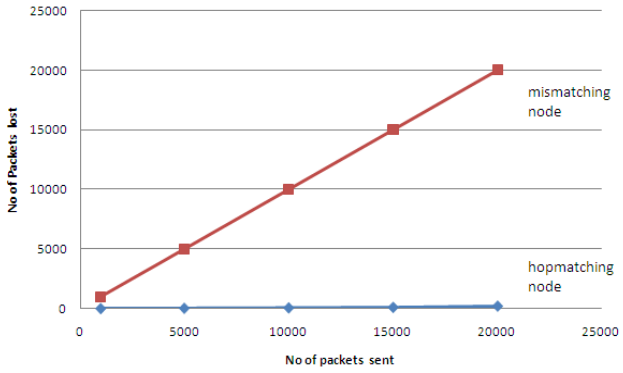

Figure 1.3: No of Packets lost

B. Hardware Measures

Zigbee p20 has been used, it has 16 channels available in entire bandwidth. It is shown in below Table 1.2.

Table 1.2 Channel availability

Channel no	Frequency Channels (In Ghz)
F1	2.405
F2	2.410
F3	2.415
F4	2.420
F5	2.425
F6	2.430
F7	2.435
F8	2.440
F9	2.445
F10	2.450
F11	2.455
F12	2.460
F13	2.465
F14	2.470
F15	2.475
F16	2.480

This proposed neighbor count based frequency hopping has been implemented in hardware. The Core of this method depends on the number of neighbors. Based on sharing count pair between two nodes the number of times frequency changeover occurs. By varying the node count the frequency variation within packets is monitored this is mentioned in the following Table 1.3.

Table 1.3: Channel hopping

Count pair	Frequency hopping (512 bits)					
1,1	F2-256			F14-256		
2,3	F7 - 96	F9 - 160		F3-176	F1 - 80	
3,2	F1- 176	F3 - 80		F7 - 96	F9 - 160	
3,3	F12 - 88	F10-88	F7-80	F3-88	F6-88	F9-80

This proposed method is a good defence against selective jamming attack. In which the, attacking node tries to overuse the intermediate node, thereby the natural data between nodes not being able to take its path. It causes jamming in network. This situation could be avoided since here nodes have no knowledge about neighbor count based and hop selection algorithm could not intrude in ongoing network.

In pseudo noise generation method, all nodes follow similar hop sequence all the time, it is highly vulnerable and risks of accessibility is high. This paper recommends that no clinching is done on similar like hopping pattern, it rather suggests having fast hopping based on the positioning and nodes present at circumstances.

References

[1] Alejandro Proanzo and Loukas Lazos "Packet-Hiding Method for preventing selective jamming", IEEE Transactions on dependable and secure computing, Vol 9, No 1,January/February 2012.

[2] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications Handbook. McGraw-Hill 2001.

[3] D. Stinson, "Something about All or Nothing (Transforms)," Designs, Codes and Cryptography, vol. 22, no. 2, pp. 133-138, 2001.

[4] TaochunWang,1,2 Xiaolin Qin,1 and Liang Liu1 "Research Article An Energy-Efficient and Scalable Secure Data Aggregation for Wireless Sensor Networks"- Hindawi Publishing Corporation International Journal of Distributed Sensor Networks,volume, 2013.

[5] J. Girao, D. Westhoff, andM. Schneider, "CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications (ICC '05), pp. 3044–3049, Seoul, Korea,May 2005.

[6] S. Ozdemir and Y. Xiao, "Integrity protecting hierarchical concealed data aggregation forwireless sensor networks," Computer Networks, vol. 55, no. 8, pp. 1735–1746, 2011.

[7] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, "Reactive Jamming in Wireless Networks: How Realistic Is the Threat," Proc. ACM Conf. Wireless Network Security (WiSec), 2011

[8] W. Xu, W. Trappe, and Y. Zhang, "Anti-Jamming Timing Channels for Wireless Networks," Proc. ACM Conf. Wireless Network Security (WiSec), pp. 203-213, 2008.

[9] M. Alicherry, R. Bhatia, and L. Li. "Joint Channel Assignment and Routing for Throughput Optimization in Multi-Radio Wireless Mesh Networks". *In Proc. ACM Mobicom*, September 2005.

[10] P. Bahl, R. Chandra, and J. Dunagan. "SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad-Hoc Wireless Networks". In Proc. ACM MobiCom, September 2004.

[11] K. Bian, J.-M. J. Park, and R. Chen. "A Quorum-Based Framework for Establishing Control Channels in Dynamic Spectrum Access Networks". In Proc. ACM MobiCom, pages 25–36, September 2009.

[12] L.-J. Chen, T. Sun, G. Yang, M. Y. Sanadidi, and M. Gerla. "Ad Hoc Probe: Path Capacity Probing in Wireless Ad Hoc Networks". In Proc. IEEE Int'l Wireless Internet Conference (WICON), pages 156–163, July 2005.

[13] A. K. Das, R. Vijayakumar, and S. Roy. “Static Channel Assignment in Multi-Radio Multi-Channel 802.11 Wireless Mesh Networks,:Issues, Metrics and Algorithms”. In Proc. IEEE GLOBECOM, November 2006

[14] Oliver Kosut, “Polytope Codes Against Adversaries in Networks” –IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 60, NO. 6, JUNE 2014.