Secure and Reliable Data Transmission in Wireless Sensor Network: A Survey

Rudranath Mitra[1], Tauseef Khan[2]
[1,2]Department of Information Technology
Heritage Institute of Technology
Kolkata – 700107.West Bengal. INDIA.

Abstract
Wireless sensor network increases its application in industrial field as well as in consumer application very rapidly. Its growth increases day by day. Sensor node normally senses the physical event from the environment such as temperature, sound, vibration, pressure etc. Sensor nodes are connected with each other through wireless medium such as infrared or radio waves it depends on applications. Each node has its internal memory to store the information regarding the event packets. Basically this whole sensor network called sensor net is working in a distributive manner, sensor nodes are deployed in a huge area and use to send data packet in broadcast manner. This data packet finally reaches to the base station or called sink and vice versa. Nodes are deployed over a huge region in an ad-hoc based manner and use to sense the physical events. If any region cannot be sensed by any nodes then that region is called blind area. If blind area is too large then data retrieval is become unreliable. Nodes normally works in a collaborative manner to perform a specific task by transferring data packet to its neighbor nodes and so on until it reached to the base station. Every node has its own transmission range and within this transmission range node can transmit data packet. The event packet which sensor node transmit may be secret or confidential for the application ; so the data transmission must be secured to maintain the confidentiality of data packets.

Key word – One way hash chain (OHC), Request for missing packet (RMP), Message authentication code (MAC), Base Station (BS).

1. Introduction

Wireless sensor network is an emerging field where lots of research work has been done involving hardware and system design, networking, security factor and distributed algorithm[1,2,3].Sensor nodes normally sense the data packet and transfer it to the base station via some intermediate nodes. The sensor nodes are low cost, low power and short transmission range [4]. Nodes use to send data packet locally to its single hop neighbor nodes and so on and finally it reaches to its base station. Initially nodes are deployed flying from aircrafts or randomly and some time node changes its initial positon (the time of deployment) and moves across the region based on the requirement; so this type of nodes is called mobile nodes. So there are two types of data transmission in wireless sensor network, these are – direct transmission and multi-hop data transmission. In direct transmission data are send directly to the sink where as multi-hop transmission data send via no of intermediate nodes lies between source node and base station. In sensor network the flow of data is very important aspect because each data packet contains the event which may be very important for some application. So data transmission must be secured. But sensor node has limited energy and limited memory capacity so maintaining security is difficult for them. [5] It should be made sure that, the reports from the '*sensors in action*' are authentic and reach the base station (BS) without any fabrication or modification. The task of securing wireless sensor networks is however, complicated because sensors are highly anonymous devices with a limited energy and memory capacity, and initially they have no knowledge of their locations in the deployment environment. To make the data transmission secure some basic aspects of security has to be maintained during transmission. Here we discussed how the authentication and confidentiality maintained during data transmission because without this two parameter data transmission cannot be reliable; also we discussed how the missing packets can be detected during transmission by some efficient methods. In this paper we will discuss various ways to make the data transmission secure and efficient; also we will discuss some mechanism and protocol used in secure data transmission.

2. Mechanism for secure data transmission

Basically to make the data transmission secure first we have to maintain two basic fields these are – Authentication and confidentiality. Authentication means it has to make sure that data packet comes from the intended sender or packet received by the intended receiver those which are involved in the transmission process. Confidentiality refers preventing the data packets from any unauthorized access.

So here we discuss a scheme which makes the data transmission secure from base station to sender node[5].One-way hash chain (OHC) and shared secret key; OHC is mainly used for authentication and secret key used for confidentiality which are pre stored at the time of deployment of nodes initially. OHC is basically series of hash function and for each data packet there is identical

hash number is generate which spread through all over the network to make data transmission authenticate. Zhu et at. [6] Proposed the interleaved hop-by-hop authentication scheme that detects false reports through interleaved authentication. Lee and Cho [6, 7] proposed an enhanced interleaved authentication scheme called the key inheritance-based filtering that prevents forwarding of false reports.

2.1 One-way hash chain (OHC) based security scheme

One way hash chain is basically used for authentication. It consists of sequence of number generated by hash function F.[8] At first base station generate a random number and then applied F on it to make the other sequence number. The first phase is used for initializing the one-way hash chain number in the network. We create a secure path from the base station to the source nodes (any sensor in the network). Along the path, the OHC plays the major role to provide authenticity of the reported data.

Assume initially all the nodes and base station are in same transmission range and each node locally broadcast its data packet to its immediate neighbor nodes. The data transmission is bi- directional that means data can be send from both side. All the sensors and the base station have shared secret keys that are pre-stored before deployment of the network. So, when the sensors are deployed in the target area randomly, each sensor contains a shared secret key with the base station. To provide data transmission authenticity, all the intermediate nodes between any source and the base station must be initialized with the basic one-way hash chain number. Let us suppose the initial hash chain number is Hs0 which is initialized by base station and it broadcast this number to all the nodes in the network.

At first base station send a control message to its one hop neighbor node which is called base station control message denoted by (bcm) . This control packet contains the initial hash number (Hs0), message authentication code (MAC) which is generated by key Ki , where ki is key generated at the time slot ti. The format of the control message is:

bcm: B|HS0|MACKi(*B*|HS0)

Here B is the id of base station.

Now this control message is send to the immediate neighbor nodes. After receiving this control message the nodes set the base station as its forwarder and add its own id and rest of the message is remain same. This control message is then again send to its one hop neighbor node denoted by (ncm). The format of this message is

ncm: sid|*fid*|*B*|HS0|MACKi(*B*|HS0)

Here sid is the node own id and fid is forwarder id which is here base station id for its immediate neighbor nodes.

Now this message is again locally broadcast by the sender nodes and received by its immediate neighbor nodes and so on. This process is continues until all the nodes in the network gets the message. If any node already got the control message then it rejects the later control message.

Now, any node that has not received the message earlier (i.e., two hops away from the base station) receives it and stores the initial OHC number, HS0. It then sets the id of the sender node as its forwarder node and again locally broadcasts the control message with its own id as *sid*. In case, it has got the control packet from two or more sender nodes, it picks up the message which it receives first and discards all other messages. However, this node stores the ids of the other senders. This knowledge is necessary to repair a broken path, which we will discuss later in this paper.

If any node set as a forwarder of any downstream nodes then eventually it knows by the bi-directional data transmission. If any downstream node already set its forwarder then it rejects other upstream immediate neighbor nodes forwarder request.

In fig (1) it shows that in this sensor network node 1, 2, 3 are the immediate one hop neighbor nodes of base station. Here total three paths which are BS-1, BS-2-4-7, and BS-3-5-6.

At first control packet send by the base station and received by the nodes 1,2,3; then data packet locally broadcast from each of the data packet. In this fig (1) node 4 set node 2 as its forwarder. Though node 4 is within the range of node 2 as well as node 3. So both nodes can send data packet by local broadcasting. But node 2 already set as the forwarder of node 4 , so node 4 rejects the request of node 3 which wants to become the forwarder. This process is maintained in the whole network.

Now node 1 and node 2 are the one-hop neighbors of the base station and they both get the control message from the same source (which is in this case the base station itself). So, when the local broadcasts of node 1 or node 2 reach each other, as previously stated they simply ignore the messages. This process continues until all the nodes in the network are authenticated using the OHC mechanism.

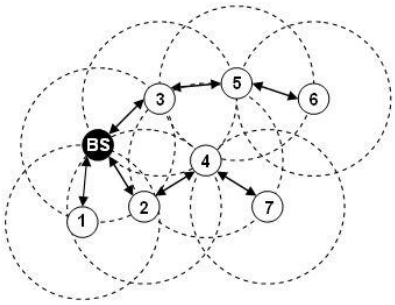

Fig (1)

So here each node locally broadcast the control message to its neighbor node which contain the hash number and authentication code and this process is continues until all the nodes are authenticated.

2.2 Secure data transmission

After initializing the hash number and getting the hash number by all the nodes which is sent by the base station now all the nodes ready to start data transfer securely. Here each source nodes maintains a unique hash chain number Hs: < Hsn.. Hsn-1.. Hs1.. Hs0 >.

it encrypts the packet with its shared secret key with the sink (or base station), includes its own id and an OHC sequence number from *HS* in the packet. It attaches HS1 for the first packet, HS2 for the second packet, and so on. To validate an OHC number, each intermediate node n1,…,nm maintains a verifier IS for each source node, ns. Initially, Is for a particular source node is set to HS0. When source node sends the *i*th packet, it includes HSi with the packet. When any intermediate node receives this packet, it verifies, if Is = *F*(Hsi). If so, intermediate node validates the packet, it forwards it to the next intermediate node, and sets Is to Hsi. In general, intermediate node can choose to apply the verification test iteratively up to a fixed number *w* times, checking at each step whether, Is = *F*(*F*…(*F*(Hsi))). If the packet is not validated after the verification process has been performed *w* times, intermediate nodes simply drops the packet.

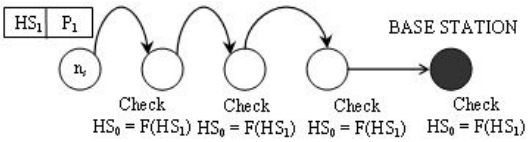

Fig (2.a)

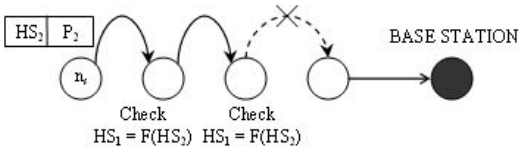

Fig (2.b)

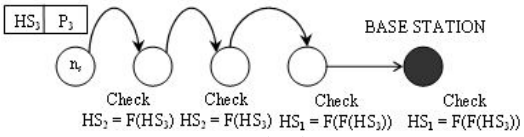

Fig (2.c)

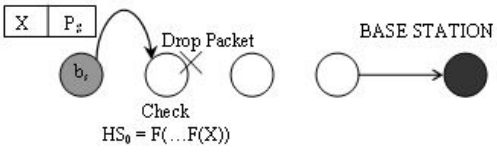

Fig (2.d)

Here it shows in fig (2) how the data are transmitted securely from source node to base station securely.
At first in fig (2.a) source node send data packet 1 along with its corresponding hash number Hs1 to the base station via some intermediate nodes. Here each intermediate node has verifier (Is) as described earlier and initially verifier set as Hs0 (Is=Hs0). At each intermediate node data packet checks for validation that is Is=F(Hs1) . If true then validation done and data packet forward to next node and again checks for validation and so on. Finally it reaches to base station. If in between any intermediate node then validation fails the data packet discarded.

Now in fig (2.b) the data packet couldn't reach to the base station because of some reason but still it doesn't hamper the data packet validation using verifier (Is). Here in this fig second data packet couldn't reach to the base station.

In fig (2.c) here node send the data packet 3 along with its corresponding hash number (Hs3). Now in previous case packet 2 with its hash number is been discarded in some intermediate node and it couldn't reach to the base station. So here data packet 3 will be verified by the verifier (Is) which is set to Hs2 up to the intermediate node which already received the previous data packet along with its hash number(Hs2) and from the intermediate node where Hs2 was discarded (in fig 2) the verifier set to Hs1 and checks the new data packet 3. So here basically two validation is done during the transmission and finally at base station two times validation is done for the received data packet. Finally in fig (2.d) source node send false packet which detects by its immediate neighbor node during validation then it immediate discarded.

So by this process data packet securely transmitted to the base station or vice versa. Source node encrypts the data packet by its shared secret key and after receiving the packet base station decrypts its by its secret key which was pre stored as stated earlier.

2.3 Optional key refreshment Mechanism for data freshness
To make the data freshness and increase the level of security another mechanism is used which is called optional key refreshment. Here base station broadcast a session key (Ks) to all nodes.
The format of this message is

$$B|\text{Ks}|\ \text{MAC}_{\text{Ks}}(B|\text{Ks}))$$

Initially this session key is encrypted by its secret key and transfer to its immediate neighbor nodes, now neighbor nodes after receiving the session key it performs X-OR operation with its own old key and form a new derived key.
This newly derived key is again used for sub sequent data packets.
So by this process every time key is getting updated and it increases the level of security every time. Because here same secret key is not used for secure data transmission, every time a newly derived key is used.

3. Mechanism for repairing the broken path in sensor network

If any intermediate node is crashed or fails to transmit then the whole path along that node is broken, all the downstream nodes get detached from the base station. So here we will use some mechanism to repair the broken path and create another alternative path to maintain the transmission of data packets.

In fig (1) if node 2 is crashed or fails to transmit data then all the downstream nodes here 4 and 7 gets detached from base station, so no data will flow along that path. This failure could first be detected by the one-hop neighbors of node 2 in the network i.e., node 4 and node 1.

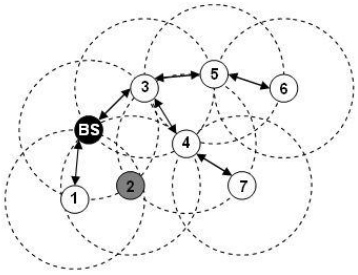

Fig (3)

Here in fig (3) it shows that node 2 is crashed or fails to send data so the entire path along that node gets down. Now to repair this broken path some technique has to be followed. Node 4 was within the range of node 2 and node 4 initially. But node 4 set

node 2 as its forwarder. Node 3 also locally broadcast the data packet to node 4 and initially wanted to become the forwarder of node 4. But node 4 rejects its request because it already set node 2 as its forwarder initially. But before rejecting the request node 4 initially in fig (1) stored the id of node 3 and also used to store other nodes id who wanted to become the forwarder of node 4. This phenomena is used to repair the broken path .Now in fig (3) node 4 has no forwarder because node 2 is crashed. So node 4 now send a message to node 3 and set it as its forwarder because initially node 4 stored the id of node 3. So in fig (3) it shows that new path has been created from Bs-3-4-7.

If node 4 is required to send any packet as a source node, it could simply send it using the OHC number in the sequence, HSk+1 which is next to its last used OHC number, that is Hsk. For node 3, node 4 is a new source, so it could save its HS value in I4. The subsequent transmissions from node 4 are verified by node 3 based on this initial knowledge.

4. Reliable data transfer with no data loss

Normally data transfer has to be reliable and make sure that no data is lost during the transmission. So there are two basic methods by which data is transfer from one node to another node reliably. This are- 1. Acknowledgement based method, 2. Non acknowledgement based method.

4.1Acknowledgement based method vs. non acknowledgement based method [9]

For both ack based and non ack based method there are three kinds of message used.

1. Transmission of data packet *pi*.
2. Acknowledgement of packet *pi* for ack based method and RMP that is request for missing Packet in non ack based method
3. Re-transmission of packet *pi* .

4.2 Acknowledgement based method

A node waits for an acknowledgement from receiver after sending the packet to receiver. It waits for a time period (*ta)*. If no acknowledgment receives within this time period then sender again re-transmits the data packet and this process continues until sender gets the acknowledgement for that data packet from receiver.

4.3 Non acknowledgement based method

In Non-ack based method sender send the first data packet to the receiver. After that it send the next data packet without waiting for acknowledgement of the previous sent data packet because here no acknowledgement is used. Now after receiving the next data packet the receiver can realize that previous data packet has not been received by the receiver; so it send a RMP request(request for missing packet) for that missing data packet. After receiving this RMP sender only send that requested data packet. So this is the main working mechanism for non-ack based method.

5. Reduction of delivery time by reducing the number of message transfer

5.1 Acknowledgement based method:

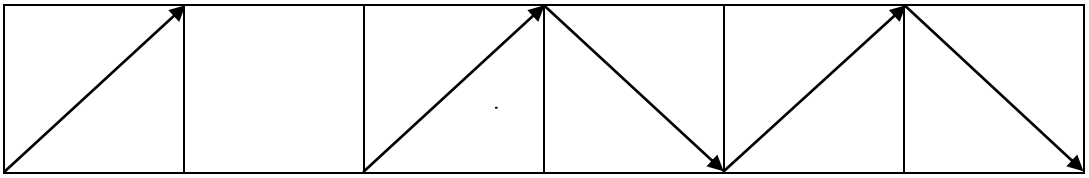

Fig (4.a)

In fig(4.a) first data packet 1 is send by the sender. Then it waits for time period (ta). After waiting for time period when sender doesn't any ack then it re-transmits the data packet. In next time slot it got then ack from receiver then sends the next data packet. Here in acknowledgement based method total no of message is five and total time slot required is 6.

5.2 Non-acknowledgement based method

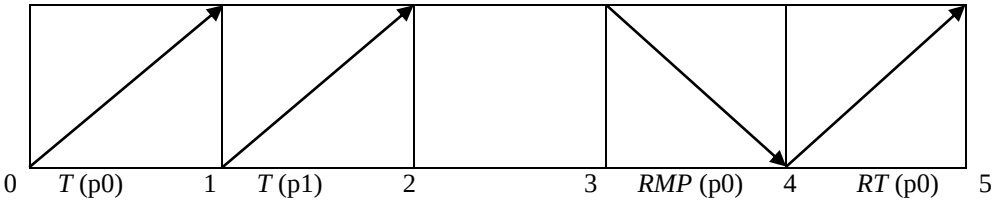

Fig (4.b)

Here it shown that in non acknowledgement based method number of message is less than Ack based method so total delivery time is is less in case of non Ack based method. Here total time slot required is 5.
So it is proved that non Ack based method takes less time to deliver packet as compare to Ack based method.

6. Comparative study:

In this paper we have studied many different methods of data transmission which are used for various aspects of data transmission. These mechanisms are used for reliability, security, detection of missing packets etc. Some mechanism is used for authentication; some maintain confidentiality to secure data during transmission etc. In this paper we basically focused on OHC and pre-stored secret key mechanism for ensuring security also optional key refreshment mechanism increase the security level by changing the session key every time. Also there are methods which are used for detecting the missing packets during transmission.
So here we are trying to compare those mechanisms by some standard parameter. So the comparison table as follows:

Mechanism	Authentication	Confidentiality	No of message deliver	Delivery time	Reliability
OHC	High	–	–	Varies	High
Pre-stored secret key	–	high	–	–	High
Optional key refreshment	High	High	–	Varies	High
Ack-based method	–	–	More	More	High
Non-ack based method	–	–	Less	Less	Low

7. Conclusion

In this paper we discussed how the data transmission can be secured and what are the main mechanisms is used to make the data transmission secure also how the broken path can be repair by re-initialization of OHC. We discussed the reliability factor in terms of data packet loss detection by these two methods. There are lots of scopes for further work on this topic also we can enhance the level of security by some new approach and reduce the delivery time by reducing more number of message transfers. Here we basically discussed how efficiently data transmission can be secured by some mechanisms. Here the optional key refreshment mechanism basically increase the level of security and ensure data freshness.
So in future there are lots of scopes to work on this field and enhance security mechanism by different methods also we can increase the reliability by reducing the no of missing packets. In future we can also work on energy efficient data transmission so the life time of each sensor node can be increased.

Acknowledgement

We express our sincere gratitude to the senior members of Faculty, Department of Information Technology, Heritage Institute of Technology, Kolkata, for extending their valuable time and guidance for the completion of this paper.

References

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", *Computer Networks*, 38, pp. 393-422, 2002.

2. S. Dai, X. Jing, and L. Li, "Research and analysis on routing protocols for wireless sensor networks", *Proc. International Conference on Communications, Circuits and Systems*, Volume 1, pp. 407-411, 27-30 May, 2005.

3. D. E. Culler, and W. Hong, "Wireless Sensor Networks", *Communication of the ACM*, Vol. 47, No. 6, pp. 30-33, June 2004

4. Yu Wang, Hongyi Wu, and Nian-Feng Tzeng ,**"**Energy-efficient Data Transmission in Wireless Sensor Networks**"**, in Center for Advanced Computer Studies University of Louisiana at Lafayette P.O. Box 44330, Lafayette, LA 70504. Email: {yxw1516, wu, tzeng}@cacs.louisiana.edu.

5. Al-Sakib Khan Pathan and Choong Seon Hong ,"An Efficient Scheme for Secure Data Transmission in Wireless Sensor Network.", in Department of Computer Engineering, Kyung Hee University spathan@networking.khu.ac.kr and cshong@khu.ac.kr.

6. S. Zhu, S. Setia, S. Jajodia, P. Ning**,** "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks**",** In *Proc. of S&P*, pp. 259-271, 2004.

7. .H. Y. Lee, and T. H. Cho, "Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks"**,** *LNCS 4317*, Spr.-Ver., pp. 116-127, 2006.

8. L. Lamport, "Constructing digital signatures from oneway function." In technical report SRI-CSL-98, SRI International, October 1979.

9. Al-Sakib Khan Pathan and Choong Seon Hong ,"Reliable and Efficient Data Transfer in Wireless Sensor Networks via Out-of-Sequence Forwarding and Delayed Request for Missing Packets",in *Computer Science Dept, Louisiana State University Baton Rouge, LA 70803, USA {ddatta1@lsu.edu, kundu@csc.lsu.edu}.*