Scientific Journal of Impact Factor (SJIF) : 3.134

ISSN (Print) : 2348-6406
ISSN (Online): 2348-4470

International Journal of Advance Engineering and Research Development

Security Analysis in Wireless Sensor Network Using Time Synchronization

Shyam Narayan Patel[1], Akash Singh Chauhan[2]

[1]School of Electronics Engineering, VIT Chennai, (T.N.) India, 1shyam.narayan2013@vit.ac.in
[2]School of Electronics Engineering, VIT Chennai, (T.N.) India, 2akash.singh2013@vit.ac.in

Abstract-*This paper proposes a security mechanism that uses a time synchronization Protocol between the base station and node. It also provides the good packet delivery ratio. In this paper we propose a security algorithm by introducing a MASTER NODE which provides the timestamp of every stage of data routing. By this approach it identifies the malicious node by using time synchronization approach. A main objective of this approach is to avoid the delay. With the time synchronization protocol it identifies the Sybil attack, and packet replay attack and denial of services attack.*

Keywords- *WSN, Cryptography, Time synchronization, Sybil attack*

I. INTRODUCTION

In a modern wireless technology improves the security of services and the growth of low power, low cost and multitasking electronic device i.e. sensor nodes. A collection of sensor node is a kind of multi-hop, dynamic, routing network and every sensor nodes are connected to a lot of powerful ancient network and resources. Within the tract police investigation application, a sensor node may monitor the handing over of vehicles and for tracking the position of enemy and also other important application like forest fire detection. Security of a network addresses these major concerns confidentiality, integrity, availability and authenticity. Cryptography is a technique, which provides the confidentiality, authentication and integrity in a sensor network as well as data network [1].

Wireless sensor network (WSN) application like military application it performed a critical task. Then it clears that security demand to be taken into consideration throughout the plan timing itself. Moreover, mostly wireless sensor network ought to run endlessly and faithfully with none interruption. Therefore incorporating security in WSN is extremely challenging. In Wireless sensor network sensor node consist of varies type of low power, low cost distributed electronic devices, and also it has both volatile and non-volatile memory to store the security related data like program, routing table and node-ID.

WSN are unprotected due to various types of attacks like packet replay attack, spoofing or modification of packet, Sybil attack, and node compromise attack and in which compromise node injected of false messages and denial of service (DoS) attacks [1].

To provide the secure communication key distribution and its management is very challenging. In this paper proposed asecurity mechanism by providing the time synchronization of each stage of communication with a master node and also used a multiple key used concept. In over The network a master node gives the acknowledgement of transferred data to the base station and in a cryptography method keys are not distributed simultaneously. Instead, some parameter are used to generated and transmit the key only during the re-keying request. It's difficult to hard by adversary of identifying that parameter.

The rest of paper is organized as follows, in section II we address the related works on security by using the secret key, and in section III describes the existing work. And we proposed security solution in a section IV, Section V we describes some conclusion.

II. RELATED WORK

In a wireless sensor network time synchronization is a critical problem over the proper data transmission across multi nodes, which has connected together. Last few year back so many researches had to overcome this, many protocols have been design and critical algorithms are also used like a time sync protocol [2], light weight time sync[3], time-synchronization protocols for sensor network, Flooding time-sync protocol [FTSP], and Tiny sync any mini sync (TM/MS).

Each type of protocols have a same basic features: an easy connectionless electronic messaging protocol, among the node clock information may exchange, a nondeterministic factor impact in a message delivery, and utilizing the processing of variant schemes and algorithms.

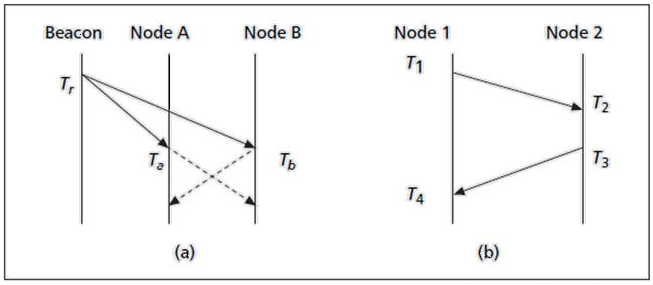

Figure 1. Sync mechanisms: (a) one directional (b) bidirectional pair wise broadcast [2]

Synchronization can be divided in two types: A bidirectional (duplex) pair-wise synchronization and one directional synchronization for broadcasting. A duplex broadcasting is called rec-rec sync. Where a node broadcasts the wireless beacons periodically to their neighbour. And the receiver usage the arrival time of message and compare at the reference point of their clock and then they exchange a local value of timestamp of as it is broadcast message they receive. And it gets the off-set based difference to synchronize its clock. This scheme is shown in figure 1(a) [2].

It compares to the standard protocols acting on a computer network. A major objective is that to contribute directly take away the transmission time and its access time of nondeterminism concerned in massage transmission through exploiting the thought of a time critical path. This is a path of message which is contributing the error of nondeterministic synchronization. So that RBS was not providing the accuracy of synchronization in a WSN [2]. A medium access control layers time-stamping is used in a FTPS and also use the disturbance reducing technique, and estimation of clock drift to realizes comparatively high precision. In a bidirectional pair wise synchronization scheme performed operation by using a handshaking protocol between the pairs of sensor node. It shows in figure 1(b). So by using in this type of protocol a Hough amount of energy and time can be loss.

In this paper propose a scheme where a master node delivered the synchronization detail to its neighbour nodes. And in also overcome the problem of above protocol based scheme.

III. EXISTING WORKS

The point should be cleared that there is a no ideal scheme for key distribution to various kind of WSN application. If keys are distributed at once for lifetime, during this keys can be hacked or modified. Therefore it batter to get the key for every rounds and once needed. CL Chen Chang and CT.Li [4] was proposed a dynamically key selection and management scheme for the WSN, where the node that needs a key, generates the key by using the last two previous keys, which are already store in a sensor node. For generating the new keys they use one way function.

Due to the security aspect the sensor node shouldn't invariably depend upon the static keys. And it is preloaded at once during the entire life time of network. So that it should have provided the rekeying facilities to repeal the key when key identified by adversaries or expired the key lifetime [6].

In many key management and distribution schemes are projected the randomly redistribution of keys scheme and pair-wise key sharing schemes. Sharing a secret key among the entire node is susceptible to attack. Instead each node will have various pair-wise key is more secure; however this technique occupies the extra spacing on a node [7]. Instead of all these kind of process, only some parameter will be predistributed that also used for generating the key [4]. Sensec [8] uses the skipjack algorithm but it introduce in a different manner, is called SKIPJAJK-XX for data encryption and decryption and cipher text generation. It also uses the secret keys on its algorithm without affecting the structure.

V. Thir. Kes. [5] Propose a multiple secret key based scheme using cryptography. In 1which they provide the secrecy of a data during transmission. A wireless network have a so many number of sensor nodes shown in figure 2. On that approach the entire node divided into individual groups based on the network size and each group has an equal number of n.

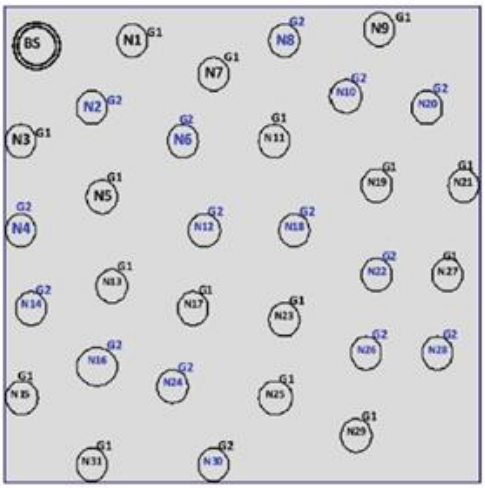

Figure 2. Network with two groups of keys [5]

In which a node wants a rekeying request than other also participated for rekeying. That approach avoids this type of difficulty. The overall security solution detail that ensure the subsequent security properties:

- Privacy: Even the adversary captured the node physically, but it can't be recovered the secret information in a node memory.
- Backward secrecy: Even the adjacent keys are recovered by the attackers; it's not possible to retrieve the previous keys.
- Data Integrity: It decides that during the transmission of data the network should not be modified by attacker.
- Secure data management: In the mechanism provide the security approach for the rekeying support as well as new key generation which is important in defensive against cryptography attacks [1].

In multiple secret key use based approach also they identified the Dos attack and Sybil attack and protect the data with the use of skipjack algorithm for encryption and decryption of the message, and also the use some kind of message authentication protocols. With protocol support node requested for rekeying facilities, if a node may be captured by adversary or it can be compromised or a key lifetime is expire. A new rekeying key was generated through a one-way hash function for communicating with a base station. On that approach three type ok keys being used:

- Data encryption key [DEKs]: group and BS station generates and share these keys.
- Rekeying key (ReK): it is shared and generated between BS and Node at during the rekeying request.
- Secret key (SK): at last stage of authentication it's used by BS and Node.

The key ReK, DEK and SK store in volatile memory of the node. Because in case a node may be captured by adversary, it can't be able to retrieve the key from the volatile memory.

IV. PROPOSED SECURITY SOLUTION

Here we are suggesting a security mechanism to identify the malicious node on a sensor network and how to overcome the energy consumption. It ensure that the following property for security.

- Sybil attack: A particular node act itself as a multiple entities are present to the network. It also acting as an original node and introduce the false tolerance or packet into the network. It disrupts the network setup and misleads the routing algorithm.
- Sink-hole attack: In this attack node act as base station and stop the message forwarding process to receiver.
- Selective-forwarding attack: Adversary captures the certain node and it does not pass the message they received.
- Wormhole attack: In wormhole attack it increases the latency. And it gives the false data to node through a very long path by making traffic of network.

When the base station sends or receives any message a master node provide the authentication between the base station and sensor node, through time synchronization. And if any malicious node present in a network, it identify that and updated the information to the base station. Base stations take an action about the selfish node and resolve the difficulty.

4.1 Goals of design: To provide the proper time synchronization in a sensor network introduce by the master node which identify malicious node and updated the information to base station. In the data routing for mainly identifying the replay attack and Sybil attacks. An initial synchronization is shown in figure 3.

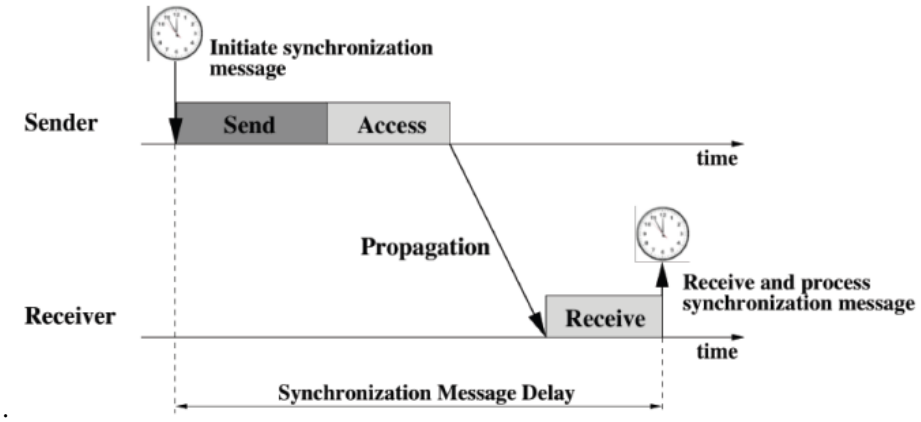

Figure 3. Time Synchronization

4.2 Node deployment: In this propose approach introduction the master mode between the centers of every node show in figure 4. That wireless network has so many numbers of nodes. In thin approach all the node divided into individual groups based on the network size. Each group has an equal number of nodes. In which a node wants a rekeying request than other also participated for rekeying. This approach avoids difficulty for that node belongs to different group(S) who's requested rekeying support.

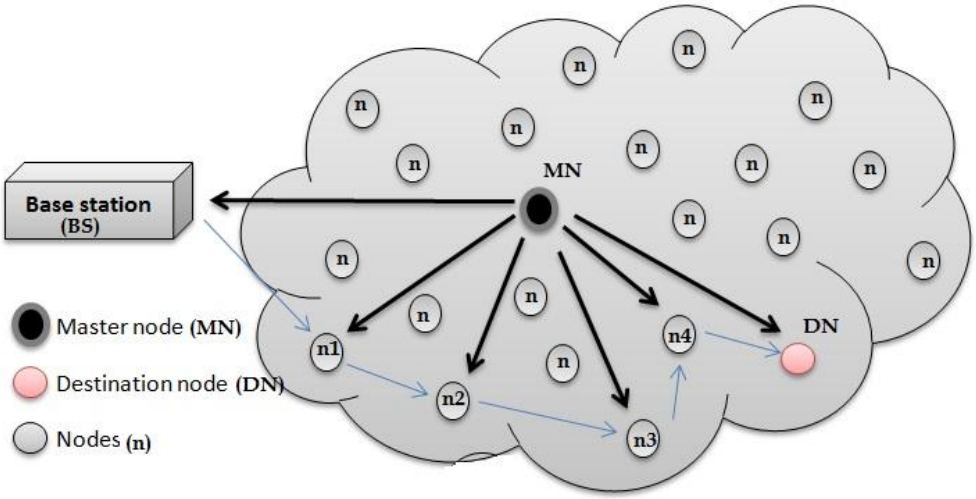

Figure 4. Network representation showing MASTER NODE.

4.3 Important parameter: Synchronization is needed to regulate the clock reading such they match.Synchronization beacons broadcasts periodically and it contain relative logic time and current logical time. Each node has routing table to bypassing the malicious node. Some kind of important parameter is used in this approach shows in figure 5.
Clock offset: it is a local time difference between a two nodes.
Clock rate: is a frequency in which clock should be progressed.
Global Clock skew: network synchronization error between the nodes present in a network.
Local clock skew:neighbour synchronization error between two adjacent nodes.

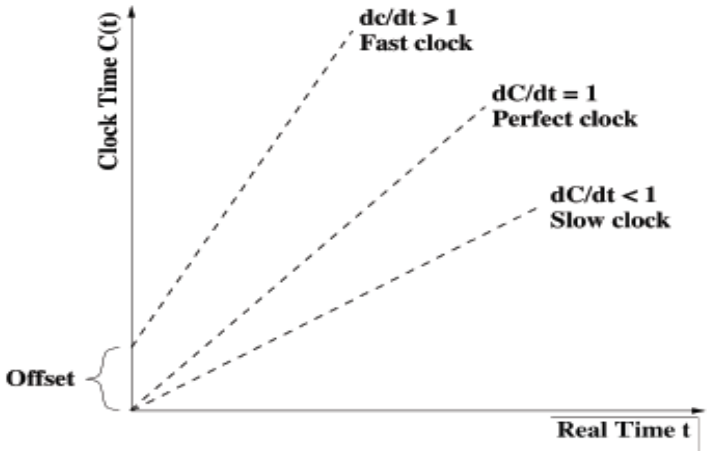

Figure 5. Clock time and Real time

4.4 Proposed Algorithm- In this approach usage of the two different algorithms for the different purpose. In a Wireless communication two basic aspects always challenging, one is the data routing i.e. which packets of data travels in entire network and other is data and entity authentication. For the secure communication symmetric key cryptography based skipjack algorithm is used for the both encryption and decryption of data [5].

This algorithm used because of in this memory requirement is less as compared to other symmetric key cryptography algorithm, also multi key storing setup is good. But the main issue is secure data routing, during the transition of data if any node can selfish or compromised by adversary; it is not pass the data to next node. So by the time synchronization it was find out the selfish node figure 6 show the flow of work done.

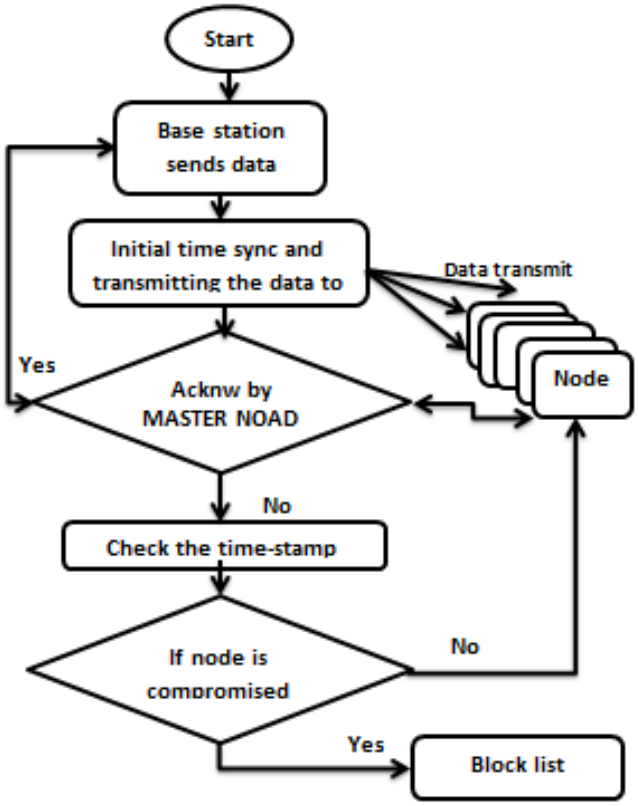

Figure 6. Flow chart of time synchronization

For the secure data routing use the proposed algorithm. Where one master is act as a leader node and it stabilized the network with a time stamping value.

4.5 Time synchronization: As mentioned bellowing various steps node and base station simultaneously send the message to each other for making a stable connection for communication.

Step 1: source node to n4.
(ScrID, grpNo, MN_ID, data, CertDN, dst_addr)
Step 2: node n4 to n3.
(ScrID, grpNo, MN_ID, data, Certn4, dst_addr)
Step 3: node n3 to n2.
(ScrID, grpNo, MN_ID, data, Certn3, dst_addr)
Step 3: node n2 to n1.
(ScrID, grpNo, MN_ID, data, Certn2, dst_addr)
Step 4: node n1 to BS.
(ScrID, grpNo, MN_ID, data, Certn1, dst_addr)

V. CONCLUSION

In a wireless sensor network all time synchronizing scheme have a common objectives to increase the lifetime of network. But in this approach it also overcomes the energy consumption. Time synchronization technique provides a very good packet delivery ratio. A grouping of node and establishment of master node does not mean that a master node communicates only in single group, it work as a leader to protect all surrounding nodes. Any node of group can send the data request. So still they so many challenges solve together. And the connectivity of master node to all other participating node, and master node also consume an extra energy is not a big issue in this scheme.

REFERENCES

[1] X. Chen, K. Makki, K. Yen, N. Pissinou, “Sensor network security: a survey”, IEEE Communications Surveys & Tutorials, Vol. 11(2), 52-73, 2009.
[2] J. Elson, L. Girod, and D. Estrin, “Fine-Grained Network Time Synchronization Using Reference Broadcasts,” Proc. 5th Symp. Op. Sys. Design and Implementation, 2002, pp. 147–63.
[3] J. Van Greunen and J. Rabaey, “Lightweight Time Synchronization for Sensor Networks,” Proc. 2nd ACM Int’l. Wksp. Wireless Sensor Networks and Apps., 2003, pp. 11–19.
[4] C.L. Chen and C.T. Li, “Dynamic Session-Key Generation for Wireless Sensor Networks”, EURASIP Journal on Wireless Communications and Networking, Vol. 2008.
[5] V. THiruppathy kesavan, and S.Radhakrishnan “Multiple secret keys based cryptography”. International journal of comm. Vol. 4, N0o.1, April 2012.
[6] L. Eschenauere and V. D. Gligor, “A key-management scheme for distributed sensor networks”, 9th ACM conference on Computer and communications security, Washington, DC, USA. 41–47, November 2002.
[7] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks, "Wireless Sensor Networks, ch.1, pp. 277-303,2004.
[8] T. Li, H. Wu, X. Wang and F. Bao, “SenSec: Sensor Security Framework for TinyOS”, Second International Workshop on Networked Sensing Systems, San Diego, USA. 145-150, 2005.

