IJCSN International Journal of Computer Science and Network, Volume 4, Issue 2, April 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Real Time Execution of Secure Time Synchronization in Wireless Sensor Networks

[1] Piyush Dhule, [2] Chetan Pise , [3] Sarika Bongade

[1] Computer Technology Department, Rajiv Gandhi College of Engineering and Research, RTMNU, Nagpur, Maharashtra, India

[2] Information Technology Department, Rajiv Gandhi College of Engineering and Research, RTMNU, Nagpur, Maharashtra, India

[3] Computer Science and Engineering Department, Rajiv Gandhi College of Engineering and Research, RTMNU, Nagpur, Maharashtra, India

Abstract - Wireless Sensor Network and security is innovative research area for some research aspirants. Time synchronization is the delicate part in the Wireless Sensor Network (WSN) due to the requirement of coordination between sensor nodes. Also security plays important role to avoid attacks on time synchronization. In this paper, we have shown necessity of secure time synchronization, problem related with synchronization, how secure time synchronization can be achieved on sink node with reduced energy consumption, quickness in effective manner. Our scheme removes different threats on synchronization and makes system more robust. We have provided centralized control in distributed wireless sensor network which reduces complexity of real time application of wireless sensor network.

Keywords - *Wireless Sensor Network, Secure Time Synchronization, Reduced Energy Consumption, Real Time, Centralized Control.*

1. Introduction

Wireless sensor network (WSN) consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. WSN is a gathering of nodes organized into a cooperative network. Each node either source node or sink node consists of processing capability may contain multiple types of memory have an RF transceiver, have a power source (e.g., batteries and solar cells), and accommodate various sensors suitable as per application. [1] Synchronization means coordination of actions between processes. Process are usually operates independent of events in other processes. Sometimes need to synchronize for mutual exclusion, for event ordering. Many of the applications of WSN needs the event with time stamp.. When WSN is energy save enabled, it need all nodes to be in sync in order to work efficiently. Affecting factors on time synchronization scheme are communication overhead, available bandwidth, Accuracy requirements, Scalability, Infrastructure Requirement [2].

In WSN, there are different threats like Malicious outside, Attacker with jamming and replay abilities, compromised node. Malicious nodes inserted in the network and sends corrupt data to the sink node which creates eavesdrop. Attackers with jamming and replay abilities can initiate pulse delay attacks. It jams a message, store, and replay later. Compromised node is friendly node taken by enemy node which creates ambiguity. To avoid such threats on synchronization there is necessity to provide secure synchronization.

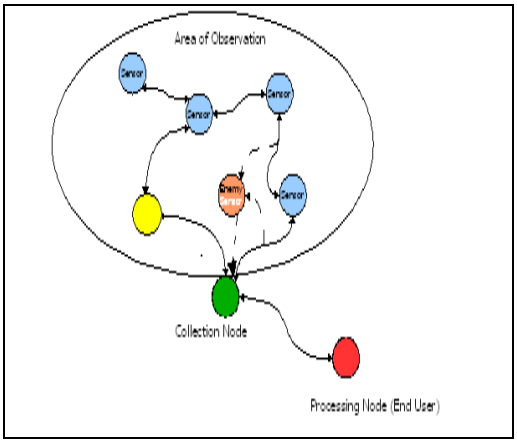

Fig. 1 Different major attacks on time synchronization

2. Related Work

In this section, we envisaged several related works from this domain. We focus on secure time synchronization protocols. There are different protocols available for secure time synchronization. In the work by Sun et al [5] , the authors propose a secure time synchronization protocol utilizing GPS devices starting from source nodes The proposed work requires a shared static key between the communicating nodes and assume that the source nodes will be equipped with GPS devices, which is more costly due to periodic communication to GPS satellites and increased radio activity increases the opportunity for malicious threats. Also, GPS may not be effective for all sensor applications (e.g., underwater medium) as explained in the previous section. Additionally, similar to [6], the nodes exchange many messages.

In [7], authors provided a secure time synchronization protocol for heterogeneous sensor networks with a novel adoption of identity-based (IBC) and pairing-based (PBC) cryptography over elliptic curves, but the work did not present any performance evaluation to provide clock precision values. Furthermore, two pertinent studies based on associating keys with time information available in sensor nodes were presented in papers.

Ganeriwal et al. proposed a suite of secure time synchronization protocols where different hop, group synchronization are addressed with a protection against pulse delay attacks [3]. However, these protocols require the nodes to go through the phase of key discovery with their preloaded static keys among themselves. Moreover, the protocols Communicates with many messages to synchronize the sensor Network with security, It increase the communication costs of the network and making them not applicable for military-type scenarios where a more feasible communication pattern may be preferred. However, the drawback of this work stems from its statistical nature [4].

In [8], a broadcast authentication scheme, µTESLA, was introduced utilizing the notions of loose-time synchronization and delayed key disclosure. However, sending keys as a separate message is not cost effective and keys may be lost due to communication errors. In fact, another worthwhile study [9] shows how TESLA would be vulnerable to attacks due to its delayed key disclosure concept. On the other hand, in Time information based Pre-deployed Secure Key Distribution (TPSKD) [10], time is used to create session keys between the communicating nodes. Several disadvantages exist in this study. First, the nodes still exchanges _i (drift) values when stabilizing a pair wise session key with each other; thus, the communication cost of the nodes is increased. Second, the scheme loads the sensors with a randomly chosen fixed _i value initially and assumes the sensors will always drift with this static value. However, in reality, nodes may have different drift values due to the effects of different environmental conditions.

In another work Secure Time Synchronization against Malicious Attacks for Wireless Sensor Networks by V. Vijayalakshmi, Dr. T.G.Palanivelu and N.Agalya proposes a technique called level-based time synchronization to provide redundant ways for each node to synchronize its clock with the common source, so that it can tolerate false synchronization data provided by compromised nodes [11].

In another work Secure Source-Based Loose synchronization (SOBAS) for Wireless Sensor Networks [12] time based key is used for secure time synchronization between source nodes and sink node. The Secure Source Based Loose Synchronization (SOBAS) protocol is used to securely synchronize the events in the network, without the transmission of synchronization control messages. SOBAS provides an effective dynamic en route filtering mechanism, where the malicious data is filtered from the network. With SOBAS, synchronization is achieved at the sink as quickly, as accurately**,** and as surreptitiously as possible. But as per our point view it is difficult to implement such scheme in real time application.

3. Secure Time Synchronization

3.1 Planned System

The technique can be effective to securely synchronize the data and source node with the sink node in the network, without transmission of synchronization control message separately. Here we focus on ensuring that each node gets synchronized with sink nodes also event ordering on sink node can be achieved and nodes along the data delivery path such that event reports is generated by the sink are ordered properly. With our scheme we are able to achieve our main goal of synchronizing events at the sink and the data delivery with quickness, accuracy, security.

In our system, we have considered nodes which can communicate with base station .Here we are using time as key for secure communication, also RC6 algorithm is used for encryption of a data in wireless sensor network. In this, different nodes of wireless sensor network firstly communicate with base station or sink node through

wireless medium using RF module, then base station sends local time as key to the nodes with the help of this key synchronization can be achieved on sink node again for secure communication RC6 encryption algorithm used for secure data delivery to the sink node ,sink node carries decryption algorithm through which original data can be obtained ,event ordering also takes place on sink node. Sink node able to send data to the outside world or other network.

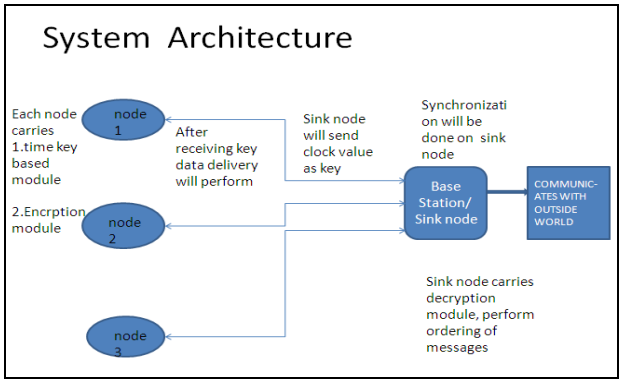

Fig. 2 Scheme of work

It will reduce energy consumption as wireless sensor network have one of the major issue of energy consumption, also with no requirement of synchronization control message it provides quickness with less delay in data delivery. Also RC6 is lightweight algorithm and good enough to provide security.

3.2 Algorithms

The algorithms used in our scheme is given as follow[13].

1. Communication establishes between nodes and sink node
2. Time based key formation done from sink node and send to the source node
3. Each source node carries encryption module using RC6 algorithm
4. Encrypted data will be deliver with obtained time key to sink node
5. If no data is send from source node then according to algorithm it will move towards next source node and so on.
6. again time key will be send to source node from sink node and data will be deliver back to sink node
7. Encryption and decryption module is present on sink node which decrypts the upcoming information.
8. These data will be arrange in order to send data to outside world

The pseudo code of the encryption algorithm of RC6-w/r/b is as followings.

1. Input: Plain text stored in four wo-bit input registers
2. E,F,G,H
3. Number of r rounds
4. wo-bit round keys S[0,…,2r + 3]
5. Output: Cipher text stored in E,F,G,H.
6. Procedure: F = F+ S[0];
7. H = H + S[1];
8. for(i=1; i<r; i++)
9. {
10. t = (B (2B + 1)) □ log w;
11. u = (D (2D + 1)) □ log w;
12. C = ((C □ u) □ t) + S[2i+1];
13. (E,F,G,H) = (F, G, H, E); }
14. E = E+ S[2r+2];
15. G = G + S[2r+3];

The pseudo code of the decryption algorithm of RC6-w/r/b is as followings.

1. Input: Cipher text stored in four w-bit input registers E,F,G,H
2. Number of r rounds
3. wo-bit round keys S[0,…,2r + 3]
4. Output: Plain text stored in E,F,G,H
5. Procedure: G = G + S[2r+3];
6. E= E+ S[2r+2];
7. for(i=r; i>=1; i--)
8. {
9. (E,F,G,H) = (H, E, F, G);
10. u = (H (2H + 1)) □ log wo;
11. t = ((2F + 1)) □ log wo;
12. G = ((G- S[2i+1]) □ t) □ u;
13. E= ((E- S[2i]) □ u) □ t;}
14. H = H - S [1];
15. F= F - S [0];

3. Hardware Infrastructure

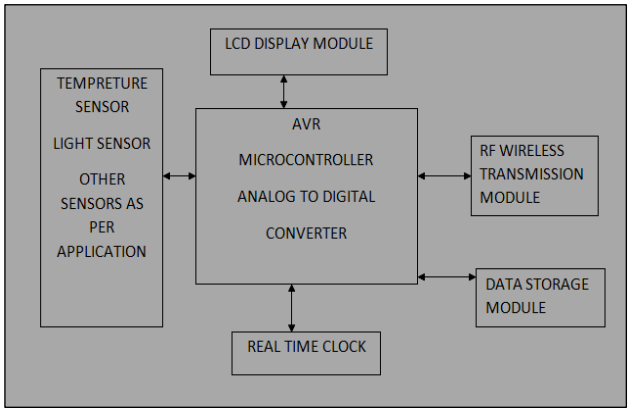

Fig. 3 Node Structure

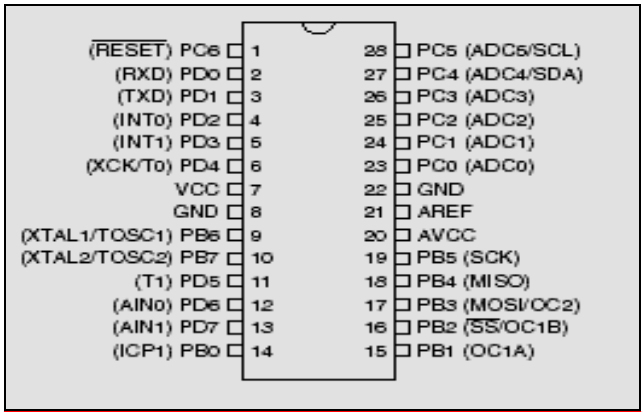

Fig. 4 Microcontroller

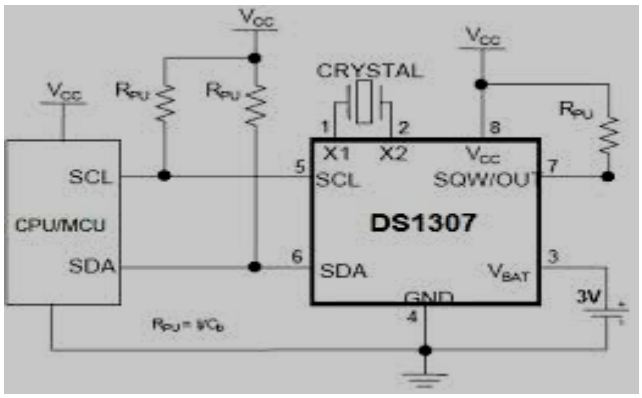

Fig 5.Real Time Clock

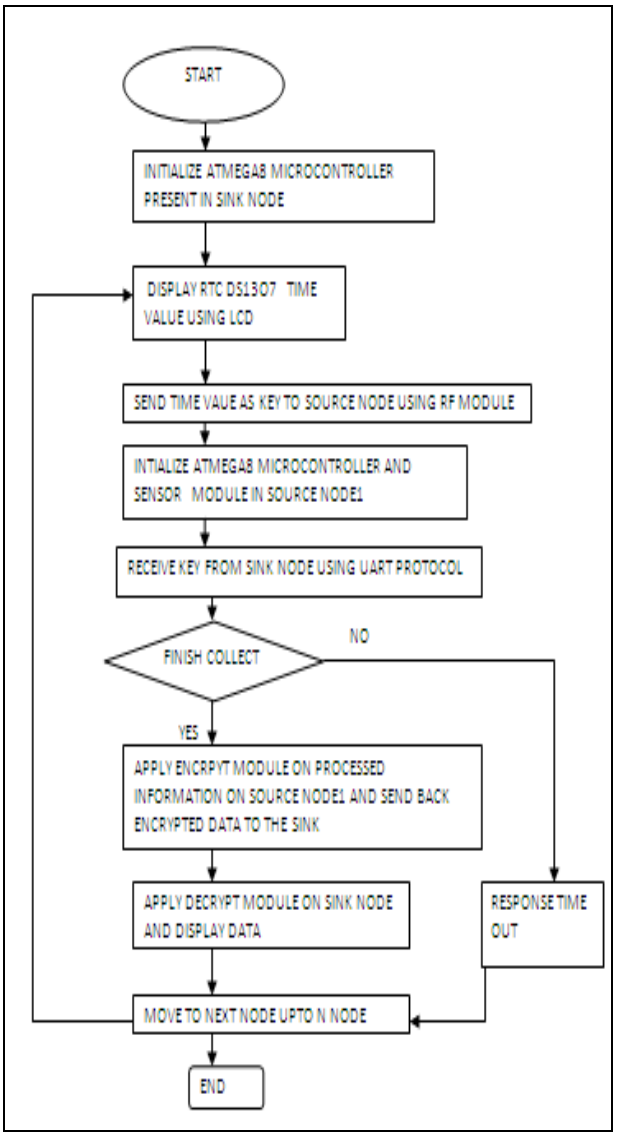

Fig.6 Flow Diagram

4. Implementation Result and Analysis

In our scheme, the Fig.3 shows how the sink node would appear. Sink node consist of real time clock through which time synchronization will be achieve. The current time of clock would send to the nodes sequentially which use as time based key for secure synchronization Source node accepts the key from sink node and using time key it sends data to the sink node similarly communication between other nodes takes place. It will reduce energy consumption because less communication message requires.

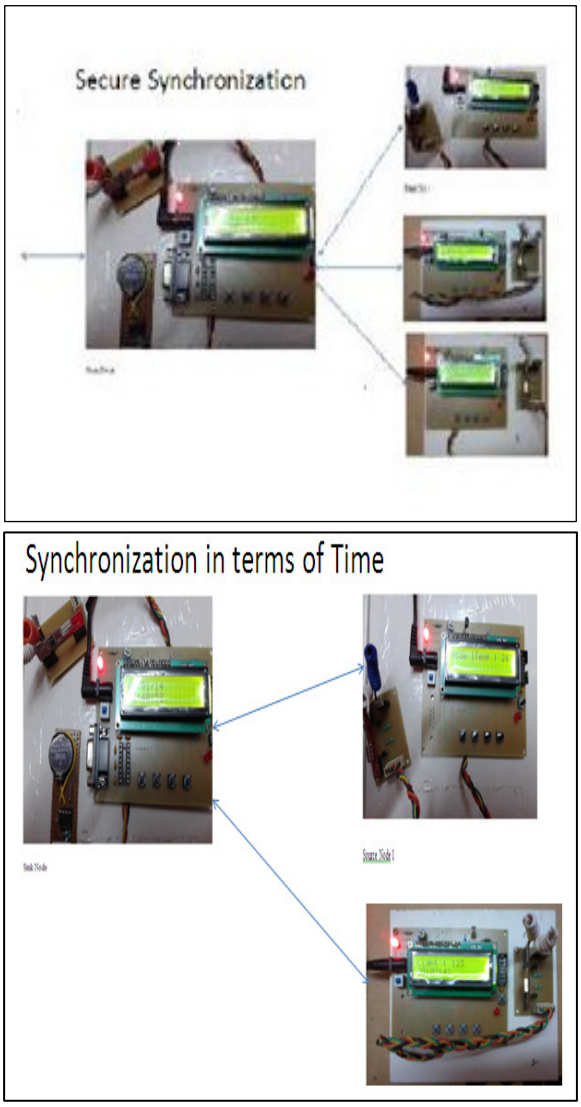

Fig. 7 Implementation Result & Analysis

4. Conclusion and Future Work

Mostly the techniques for secure time synchronization send different synchronization messages, in some techniques static pair wise key-based cryptographic mechanisms is used in order to provide secure synchronization. Some techniques uses GPS, sensor nodes have resource limitation, also data transmission cost is significant in wireless sensor networks. We tried to overcome such problem and provided secure synchronization in WSNs. We have focused on reducing the communication overhead in the network so that the energy requirement reduces and that energy can be use for security purpose. In this system, ordering of message is achieved .Moreover, In this, local time value is used as key for security.. With this, we are able to provide synchronization at the sink as quickly, correctly and securely as possible. Also it reduces the opportunities for malicious threats to eavesdrop, intercept packets, etc., by reducing the number of messages interchanged. Thus, energy saved from the reduced transmission will be use for the security. Compromised nodes as threat are not under consideration in this scheme, in future, it can be done with new techniques.

Acknowledgment

This system work is supported by my seniors, some experienced personalities. I am very thankful to those who provide me guidance and make this task reachable**.**

References

[1] International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 3, September 2012

[2] S. Ganeriwal, C. P¨opper, S. ˘Capkun, and M. B. Srivastava, “Secure time synchronization in sensor networks,” *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 4, pp. 1–35, 2008.

[3] H. Song, S. Zhu, and G. Cao, “Attack-resilient time synchronization for wireless sensor networks,” *Ad Hoc Networks*, vol. 5, pp. 112–125, 2005.

[4] K. Sun, P. Ning, and C. Wang, “Secure and resilient clock synchronization in wireless sensor networks,” *IEEE JSAC*, vol. 24, no. 2, pp.395–408, Feb. 2006

[5] S. Ganeriwal, C. P¨opper, S. ˘Capkun, and M. B. Srivastava, “Secure time synchronization in sensor networks,” *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 4, pp. 1–35, 2008

[6] S. Mizanur Rahman, N. Nasser, and T. Taleb, “Secure timing synchronization for heterogeneous sensor network using pairing over elliptic curve,” *Wireless Communications and Mobile Computing*, 2009.

[7] Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “Spins: security protocols for sensor networks,” *Kluwer Wireles Networks*, vol. 8,no. 5, pp. 521–534, 2002.

[8] D. Scott, “Relying on time synchronization for security in ad hoc networks,” in *Proc. of 43rd ACM Southeast Conference*, March 2005

[9] J. Jeong and Z. Haas, “Predeployed secure key distribution mechanisms in sensor networks: current state-of-the-art and a new approach using time information,” *IEEE Wireless Communications*, vol. 15, no. 4, pp.42–51, Aug. 2008.

[10] Vijayalakshmi, Dr. T.G.Palanivelu and N.Agalya “Secure Time Synchronization against Malicious Attacks for Wireless Sensor Networks” Department of

Electronics and Communication Engineering, Pondicherry Engineering College

[11] A.Selcuk Uluagac_ Raheem A. Beyah† John A. Copeland "Secure SOurce-BAsed Loose Synchronization (SOBAS) for Wireless Sensor Network" *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, VOL. 24, NO. 4, APRIL 2013

[12] RC6-by-Morgan-Monger-2004-Fall http://www.docshut.com/hohohohohohohohor/Morgan.html

[13] B. A. Forouzan, *Data Communications and Networking (4th edition)*.McGraw-Hill, 2007.

[14] L. Lamport and P. Melliar-Smith, "Synchronizing clocks in the presenceof faults," *J. ACM*, vol. 32, no. 1, pp. 52–78, 1985

[15] R. V. et al., "Encryption overhead in embedded systems and sensor network nodes: modeling and analysis," in *Proc. of ACM CASES '03*,2003, pp. 188–197

[16] E. S. D. Guimaraes, G.; Souto and J. Kelner, "Evaluation of security mechanisms in wireless sensor networks," in Systems Communications Proceedings, 2005

[17] S. Meulenaer, Gosset and Pereira, "On the energy cost of communication and cryptography in wireless sensor networks."

[18] Yin, Qi, Fu, "ASTS: An agile secure time synchronization protocol for wireless sensor networks," in Wireless Communications, Networking and Mobile Computing, 2007.

.