International Journal of Computer Systems (ISSN: 2394-1065), Volume 02– Issue 03, March, 2015
Available at http://www.ijcsonline.com/

Energy Efficient approaches and strategies for Wireless Sensor Network

Namita Jain[A], Manju Mandot[B]

[A]Computer Science and Engineering, Mewar University, Chittorgarh, India
[B]Associate Professor, J.R.N.Vidyapeeth, Udaipur, India

Abstract

Wireless Sensor Networks (WSN) are large scale networks of sensors running on wireless environment. Wireless Sensor Networks (WSN) have specific constraints and rigorous requirements in contrast to traditional wired and wireless computer networks. Among these specific requirements, energy-efficiency is the most prominent one. The major problem in Wireless Sensor Networks (WSN) is to maintain flawless communication sharing and to ensure a reliable treatment of information. Time synchronization protocols provide a mechanism for synchronizing the local clocks of the nodes in a sensor network. Some of the sensor nodes may be malicious, which can disrupt the normal operation of a sensor network. In this paper, we find out malicious nodes and propose time synchronization based secure protocol which is energy efficient for a group of non-malicious nodes.

Keywords: *Wireless Sensor network; energy efficiency; Clock Synchronization; RBS; TPSN; Time Synchronization.*

I. INTRODUCTION

Time-synchronization is a vital element of sensor networks infrastructure, in which clocks synchronize with each other or by global time using a common reference. Furthermore, it can be used by power saving schemes to improve network life time. Present work is mainly focussed upon the assumption that by reducing transmission rate we can improve upon energy used by a network to prolong its life time. This is significant issue in energy limited Wireless Sensor Networks (WSN) [1]. They work well in WSN but energy-efficiency is not often significant design consideration. Our goal is to make it energy-efficient with proper time synchronization. We can use traditional sender-receiver sync method or receiver-receiver method to keep the clocks ticking. Another protocol Secure Pairwise Synchronization Protocol is used here To detect attacks on pairwise time synchronization message integrity and authenticity are ensured through the use of Message Authentication Codes (MAC) and of a key which is shared between them. This prevents external attackers from modifying values in the synchronization pulse or in the acknowledgement packet, without being detected. The Secure Pairwise Synchronization Protocol (SPS) requires preshared keys or a secure way to establish keys , which limits its use in environments.

The rest of the paper is organized as follows: In Section II we survey the existing time synchronization. Related work is shown in Section 2 [2]. An approach for the proposed protocol is given in Section 3 and Conclusion and Future Work made in Section 4 and Section 5 respectively.

II. EXISTING SYNCHRONIZATION METHODS AND THEIR PROTOCOLS

A. Receiver-Receiver Protocols:Reference Broadcast Synchronization(RBS):

In receiver-receiver based synchronization, sender sends message to more than one receiver and then exchange of messages take place between receivers to synchronize each other and compute their offsets based on the difference in reception time. Sender does not take part in the synchronization. Reference Broadcast Synchronization (RBS) protocol [3] is based on receiver - receiver synchronization which reduces some uncertainty of packet delays.

RBS does not consider about sender's nondeterministic packet delays: send time and access time. To remove sender's nondeterministic packet delays, RBS provides high precision of time synchronization. There are four main sources of delays that must be accounted for to have accurate time synchronization:

1. Send Time: It is that of the sender constructing the time message to transmit on the network.
2. Access Time: It is due to the MAC layer delay in accessing the network. This could be waiting to transmit in a TDMA protocol.
3. Propagation Time: The time for bits to be physically transmitted on medium is considered the propagation time.
4. Receive time: It is the receiving node processing the message and transferring it to the host.

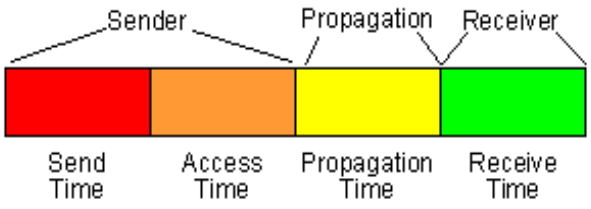

Fig. 1 Breakdown of packet delay components

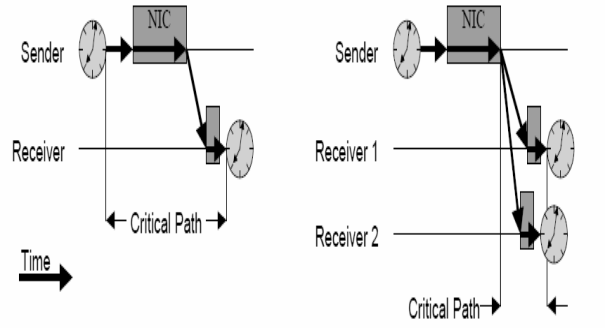

Fig. 2. Time-critical path for traditional protocols (left) and RBS protocol (right)

Above Fig 1 shows time critical path for traditional protocol and with RBS protocol. In RBS a reference message is broadcast to two or more receivers on the network and then receivers try to synchronize their local clocks respectively. Each receiver records its local time when it gets the reference message. Then receivers exchange their local times [4].

B. Sender-Receiver Protocols:

In sender-receiver approach all receivers should be synchronize with sender. Sender receiver approach basically includes three steps:
1. The sender node periodically sends a message with its local time as a timestamp to the receiver.
2. The receiver then synchronizes with the sender using the timestamp it receives from the sender.
3. The message delay between the sender and receiver is calculated by measuring the total round-trip time from the time a receiver requests a timestamp until the time it actually receives a response.

1. Timing-sync Protocol for Sensor Network (TPSN):

An alternative approach to synchronization is Timing-sync Protocol for Sensor Networks (TPSN) that aims at providing network-wide time synchronization in a sensor network [5]. It initially creates a spanning tree of the sensor network. The tree starts at the root of the network, which is generally a base station, and each node establishes its level based on the 'level discovery' message that it receives. While the tree is being built, the nodes perform pair-wise synchronization along the edges of the tree. Each node exchanges synchronization messages with its parent in the spanning tree. By comparing the reception time of the packets with the time of transmission, which is placed on the packet by the parent, the node can find and correct for its own phase offset. TPSN is a hierarchical algorithm of Transmitter-receiver type which works on two different phases. In the first step, a hierarchical structure is established in the network and then a pair wise synchronization is performed along the edges of this structure to establish a global timescale throughout the network. Eventually all nodes in the network synchronize their clocks to a reference node.

1. **Level Discovery Phase:** This is a very similar approach to the flooding phase in RBS, where a hierarchical tree is established beginning from a root node.
2. **Synchronization Phase:** In this phase, pair-wise synchronization is performed along the edges of this structure to establish a global timescale throughout the network between each transmitter and receiver.

TPSN roughly gives better performance as compared to Reference Broadcast Synchronization (RBS) and verify this by implementing RBS on motes. The synchronization accuracy does not degrade significantly with the increase in number of nodes being deployed, making TPSN completely scalable.

2. Flooding Synchronisation Time Protocol: FTSP

This protocol is similar to TPSN, but it improves on the disadvantages to TPSN. It has a structure with a root node and that all nodes are synchronized to the root. The root node will transmit the time synchronization information with a single radio message to all participating receivers [6]. The message contains the sender's time stamp of the global time at transmission. The receiver notes its local time when the message is received. Having both the sender's transmission time and the reception time, the receiver can estimate the clock offset. The message is MAC layer time stamped, as in TPSN, on both the sending and receiving side. To keep high precision compensation for clock drift is needed for which linear regression is used. FTSP was designed for large multi-hop networks. The root is elected dynamically and periodically reelected and is responsible for keeping the global time of the network. The receiving nodes will synchronize themselves to the root node and will organize in an ad hoc fashion to communicate the timing information amongst all nodes. The network structure is mesh type topology instead of a tree topology as in TPSN.

3. Secure Pair-wise Synchronization (SPS):

Secure pair-wise synchronization (SPS) is a sender-receiver based approach. Here security mechanism is integrated to make it resilient to adversarial attacks from external attackers [7]. In this protocol, message integrity and authenticity are ensured through the use of Message Authentication Codes (MAC) and a key KAB [8,9,10] shared between A and B. This prevents external attackers from modifying any values in the synchronization pulse or in the acknowledgement packet. Furthermore, the attacker cannot assume an identity of node B as it does not hold the secret key KAB. An attacker can hear the packet over the wireless channel and can use the MAC in future to generate authenticated packets. In SPS, pulse delay attacks are detected through a comparison of the computed

message and with the maximal expected message delay. If the computed delay is greater than the maximal expected delay, we recognize that there is replay on packet.

The above synchronization protocols are basically used for sensor networks. By using both sync methods (i.e., receiver- receiver and sender-receiver) we can save significant energy to sync a given network.

III. Related Work

Researchers have proposed many protocols for the time synchronization based on classification receiver-receiver [11,12] and sender-receiver [11,13]. For discussion we have considered reference broadcast synchronization [4] protocol and time synchronization protocol for sensor network [5] as receiver-receiver based protocols. On the other hand, secure pair-wise synchronization (SPS) protocol is considered as sender-receiver based protocol.

In receiver-receiver based synchronization, sender sends message to more than one receiver in the network and all receiver nodes record the receive time locally then exchange of the messages take place between receivers to synchronize each other and compute their offsets based on the difference in reception time. The information possessed by a node can be used to synchronize its' clock. This property makes it infeasible when there is large number of receivers. Sender does not take part in the synchronization.

On the other hand, in sender-receiver based synchronization protocol, the sender node periodically sends a message with its local time as a timestamp to the receiver. The receiver then synchronizes with the sender using the timestamp it receives from the sender. The message delay between the sender and receiver is calculated by measuring the total round-trip time, from the time a receiver requests a timestamp until the time it actually receives a response.

IV. Energy-aware approaches and strategies

In the paper, we have proposed an approach to develop a protocol that not only finds malicious node(s) but also counts them within the group. Also, it synchronizes all non-malicious nodes to a common clock i.e. one of the fastest clock in the group.

Let us assume that group membership is known to all group nodes in the group and all group nodes reside in each other's power ranges. Let us consider Gs is a sender node which is a non- malicious and not considered in a group. The sending time of the packet at node Gs is represented by Ts (time measured by node Gs) and receiving time of packet by node Gj is Tj (already sent by node Gs). These times are measured by two different clocks. Ts is measured in the local clock of node Gs (i.e. Cs) whereas Tj is measured by the local clock of node Gj (i.e. Cj). The offset (or the difference between the local clocks) between the two nodes is represented by δsj (calculated by node Gj with respect to node Gs). The delay for the packet transfer from Gs to Gj is represented by dsj. In proposed protocol we have assumed that a node is said to be malicious, if it does not report the exact time at which it receives or sends the packet. Herein, we assume that malicious node [14] does not report the exact time at which it receives the packet.

Steps of Proposed Protocol :

The proposed protocol has following six steps:

Step 1: Node Gs sends packets containing its node identifier (ID) and challenge nonce (Ns) to all group members. If there are N nodes in the group then in the first step the number of messages transmitted is N. In proposed protocol the initiator node is taken as sender node.

Step 2: In this step of the protocol, every node Gj, which have received the challenge packet acknowledges back to sender node Gs, known as response packet. This packet contains triples {Tj, Ns, Gs}, where Tj is the receipt time of the challenge packet from node Gi, Ns is nonce by sender and Gs is node-id of sender respectively. It also contains Message Authentication Code (MAC), which enables Gs to authenticate the packet sent by Gj in this step. The response packet also includes the sending time (T'j) from node Gj. MAC is used to provide resiliency against external attacker. So in this step N MACs are calculated one for each Gs and Gj pair and then each Gj sends messages to Gs. A pair wise secret key (Ksj) which is shared between nodes Gs and Gj is also used in the response messages.

Step 3: Now node Gs calculates the delay occurred (dsj), corresponding to challenge response and if all the calculated delays for each node are less than a maximal delay (d*) then node Gs calculates the offset for each node Gj. If any node's calculated delay is more than maximal delay then Gs assumes that Gj is external attacker.

Step 4: Node Gs will calculate for every other node, Gj, in the group Ssj (Ssj is sent time of packet from node Gs to Gj) and Rjs (Rjs is received time of packet from node Gj to Gs). If Gj is malicious then Ssj should not be equal to Rjs. This step also calculates number of internal attackers.

Step 5: Sender forms a circular path, P, of all remaining non-malicious nodes and calculate sum of all offsets along the path P. If this sum is zero, it synchronizes every node of the path P to the fastest clock.

Step 6 The final step finds malicious node(s) and also counts them within the group. Also it synchronizes these non-malicious nodes to a common clock in the group.

The proposed protocol is secure against internal as well as external attacks and can synchronize non-malicious nodes to the fastest clock in the group. We have developed three theorems in support of proposed protocol which are as follows :

Theorem 1: Prove that if at least one node is malicious in the group, nodes cannot be synchronized to the fastest clock.

Proof: A node is said to be malicious, if it does not report the exact time at which it receives or sends the packet.

Herein, we assume that malicious node do not report the exact time at which it receives the packet.

Let us consider node G_j as malicious. Here, we have assumed that malicious node do not report the exact time at which it receives the packet. Therefore, instead of T_j, node G_j will send receiving time of challenge packet as time T''_j in response packet. As we know, in non-malicious environment, sending time of the packet must be equal to receiving time of packet (since nodes are directly linked to each other in a group).

$|T_j-T_i|=|T'_i-T'_j|$

Now, since node Gj sends receiving time of packet T''_j instead of T_j. $T_j \neq T''_j$

Therefore, G_i will calculate
$|T''_j-T_i|\neq|T'_i-T'_j|$

Hence, G_j will be identified as malicious node by node G_i, and, therefore G_i and G_j cannot be synchronized to the fastest clock.

Hence Proved.

Theorem 3: Prove that using algorithm for proposed protocol one can find N-1 internal attacker(s) in the group size of N nodes.

Proof: It is assumed that, the group is made up with the help of N nodes and each node is directly connected to all other nodes in the group. Therefore, N(N-1))/2 edges exists. Assume that node G_i is non-malicious.

Now, let us consider
S_{ij}= send time of packet from node G_i to G_j.
R_{ji}= receive time of packet from node G_j to G_i.

CASE A: When there are two nodes (N=2) in the group**:**
In the group of size two nodes. If $| S_{ij} |\neq| R_{ji} |$, then node G_j is malicious. Hence, G_j will be identified as malicious node therefore G_i and G_j cannot be synchronized to the fastest clock.

CASE B: When there are three nodes (N=3) in the group**:**
In the group of size three nodes.
If $| S_{ij} |\neq| R_{ji} |$, then node G_j is malicious.
If $| S_{ik} |\neq| R_{ki} |$, then node G_k is malicious.
If $|S_{ij}|\neq|R_{ji}|$ and $|S_{ik}|\neq|R_{ki}|$ then nodes G_j and G_k both are malicious.
Hence, if N=3, then at most two nodes (G_j and G_k) can be identified as malicious nodes.
From above, the hypothesis is true for N=2 and N=3.
Now, we will prove theorem using Principal of Mathematical Induction.

Induction Hypothesis:
It suggests that P(k)=(k-1) internal attackers are identified for N=k nodes (a)
Induction step: Now we have to show that (a) is true for $N=k+1$ i.e. $P(k+1)=k$ internal attackers can be identified for $N=k+1$.

Consider there are k nodes in the group having node G_i as non-malicious node.
Now consider one new node *G(k+1).*
If $|Si(k+1)|\neq|R(k+1)i|$, then node $G(k+1)$ is malicious. (b)

Hence, from hypothesis steps (a) and (b) it can be concluded that there exists k malicious nodes in the group of $(k+1)$ nodes. Therefore, $P(k+1)$ is true. This shows that at most k nodes can be identified as malicious in group of $(k+1)$ nodes.
Hence Proved.

V. CONCLUSION

Our algorithm uses simple technique to give significant improvement over compared schemes. We improvise upon the fact that past time synchronization techniques do not take energy efficiency as important design parameter. We showed that existing solutions for time synchronization in sensor networks are not resilient to malicious behavior from external attackers or internally compromised nodes. The external attacks can be resolved with the help of MAC message authentication codes and the use of private keys. Internal attacks which occur in case of group wise synchronization can't be resolved completely and efficiently by the existing protocols till date. Further, the proposed protocol also finds out whether a nodes are malicious or not and also counts number of malicious nodes in the group.

VI. FUTURE WORK

Synchronization on nodes depends on packet transfer among nodes which consumes energy. The proposed protocol can further be modified to reduce the communication overhead, so that energy consumption can further be reduced.

REFERENCES

[1] Jeremy Elson, Kay Romer, "Wireless Sensor Networks: A New Regime for Time Synchronization", *In Proceedings of the First Workshop on Hot Topics in Networks (HotNetsI), Princeton*, New Jersey, USA. , October 2002

[2] Cayirci, E., Akyildiz, I.F., Su, W., Sankarasubramaniam, Y.: A Survey on Sensor Networks. IEEE Communications Magazine, 102–114 (2002).

[3] 3Estrin, D., Elson, J., Girod, L.: Fine-grained network time synchronization using reference broadcasts. In: Proceedings of the 5th Symposium on Operating Systems Design and Implementation Special Issue, Boston, pp. 147–163 (2002)

[4] Simon, G., Kusy, B., Ledeczi Maroti, M.: A Clock synchronization for wireless sensor networks: A Survey. In: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, pp. 30–49 (2004)

[5] Srivastava, M.B., Kumar, R., Ganeriwal, S.: Timing-sync protocol for sensor Networks. In: Proceedings of the First ACM Conference on Embedded Networked Sensor Systems, Los Angeles, CA, pp. 138–149 (2003)

[6] M. Maroti, B. Kusy, G. Simon, and A. Ledeczi, "The flooding time synchronization protocol," in SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems. New York, NY, USA: ACM Press, 2004, pp. 39–49.

[7] Manzo, M., Roosta, T., Sastry, S.: Time synchronization attacks in sensor networks. In:Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 107–116 (2005)

[8] Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks In: Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, pp. 41–47 (2002)

[9] Chan, H., Perrig, A., Song, D.: Random key predistribution scheme for sensor networks. In: Proceedings of the 2003 IEEE Symposium on Security and Privacy, p. 197 (2003)

[10] Hwang, J., Kim, Y.: Revisiting random key pre-distribution schemes for wireless sensor networks. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington DC, USA, pp. 43–52 (2004)

[11] 11Li, H., Chen, K., Wen, M., Zheng, Y.: A Secure Time Synchronization Protocol for Sensor Network. In: Washio, T., Zhou, Z.-H., Huang, J.Z., Hu, X., Li, J., Xie, C., He, J., Zou, D., Li, K.-C., Freire, M.M. (eds.) PAKDD 2007. LNCS (LNAI), vol. 4819, pp. 515–526. Springer, Heidelberg (2007)

[12] Wang, C., Ning, P., Sun, K.: Secure and resilient clock synchronization in wireless sensor networks. IEEE Journal on Selected Areas in Communications 24(2), 395–408 (2006)

[13] Song, H., Zhu, G.C.S.: Attack-resilient time synchronization for wireless sensor networks. In: IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, p. 772 (2005)