ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

ENERGY AWARE SECURITY MECHANISM IN WIRELESS SENSOR NETWORK WITH MOBILE SINK

Sathiyaseelan Rathinavel[1] and Vijayakumar P[2]
[1]Research Scholar, Department of Computer Science and Engineering,
[1]Anna University, Chennai, Tamil Nadu, India.
[2]Assistant Professor, Department of Computer Science and Engineering,
[2]University College of Engineering Tindivanam, Tamil Nadu, India.
Email: sathiyaseelanrec@gmail.com

Received on: 03-02-2017 *Accepted on: 12-03-2017*

Abstract

Providing security in a cost efficient way is the major problem in Wireless Sensor Network because of resource limited sensor devices. Therefore, the energy of the sensor node is considered while providing security. Wireless sensor network with mobile sink is vulnerable to replication attack. To avoid replication attack, the dynamic polynomial pool based key predistribution scheme is already there. But in that, energy of the sensor node is not considered. The proposed scheme provides the security with the awareness of residual energy of the sensors. The sensed information is encrypted by using the RSA algorithm. The key generated by RSA algorithm is dynamically changed for each and every packet. The energy based dynamic key generation algorithm is used o generate the dynamic key while the sensor node is in the demand to transmit the data packet. The mobile sink is aware of the residual energy of the sensors. So, based on the residual energy of the sensor, the mobile sink sends the data request. As the key is dynamically changed, the adversary cannot introduce replicated node in the network.

Introduction

Wireless Sensor Networks (WSNs) can be used in a broad range of applications, such as, military sensing and tracking, health monitoring, data acquisition in hazardous environments, and habitat monitoring. The data sensed by the sensor frequently need to be sent back to the Base Station (BS) for analysis [1]. If the distance between the sensor node and the BS is too long, then the sensor node transmits the data via multiple hops. It may weaken the security; the energy consumed by the nodes nearby BS is increased, reducing the lifetime of the network. So, mobile sinks (MSs) are important components in the process of many sensor network applications, including data collection in dangerous

environments localized reprogramming, oceanographic data collection and military navigation [2]. From a security standpoint, it is very important to provide authentic and accurate data to surrounding sensor nodes and to the sink to trigger time-critical responses. Protocols should be resilient against false data injection in the network by malicious nodes [3]. Otherwise, consequences for propagating false data or redundant data are costly, depleting limited network resources and wasting response efforts. However, securing sensor networks poses unique challenges to protocol builders because these tiny wireless devices are deployed in large numbers, usually in unattended environments, and are severely limited in their capabilities and resources. There are two fundamental key management schemes for WSNs: static and dynamic. In static key management schemes, key management functions are handled statically. The sensors have a fixed number of keys loaded either prior to or shortly after network deployment. On the other hand, dynamic key management schemes perform keying functions either periodically or on demand as needed by the network. The sensors dynamically exchange keys to communicate. Although dynamic schemes are more attack resilient than static ones, one significant disadvantage is that they increase the communication overhead due to keys being refreshed or redistributed from time to time in the network [4]. There are many reasons for key refreshment, including: updating keys after a key revocation has occurred, refreshing the key such that it does not become stale, or changing keys due to dynamic changes in the topology. The intend of this paper is to minimize the overhead associated with refreshing keys to avoid them becoming stale. The communication cost is the most dominant factor in a sensor's energy consumption [5], the message transmission cost for rekeying is an important issue in a WSN deployment. Furthermore, for certain WSN applications, it may be very important to minimize the number of messages to decrease the probability of detection if deployed in an enemy territory. That is, being less "chatty" intuitively decreases the number of opportunities for malicious entities to eavesdrop or intercept packets [6]. The purpose of this paper is to develop an efficient and secure communication framework for WSN applications. In this paper, Energy based secure communication framework is introduced that provides a technique to verify data in line and drop false packets from malicious nodes, thus maintaining the health of the sensor network. Energy aware security scheme dynamically updates keys without exchanging messages for key renewals and embeds integrity into packets as opposed to enlarging the packet by appending Message Authentication Codes (MACs). Each sensed data is protected using a simple encoding scheme based on a permutation code generated with the RSA encryption scheme and sent toward the sink. The key to the encryption scheme dynamically changes as a function

of the residual virtual energy of the sensor, thus requiring no need for rekeying. Therefore, a one-time dynamic key is used for one message generated by the source sensor and different keys are used for the successive packets of the stream. The nodes forwarding the data along the path to the sink are able to verify the authenticity and integrity of the data and to provide non repudiation.

The contributions of this paper are as follows:

- A dynamic en route filtering mechanism that does not exchange explicit control messages for rekeying.
- Provision of one-time keys for each packet transmitted to avoid stale keys.
- A robust secure communication framework that is operational in direct communication and over unreliable medium access control layers.

Proposed System

The virtual energy-based keying module of the energy aware security scheme framework is one of the primary contributions of this paper. It is essentially the method used for handling the keying process. It produces a dynamic key that is then fed into the crypto module. In Energy aware security scheme, each sensor node has a certain virtual energy value when it is first deployed in the network. The rationale for using virtual energy as opposed to real battery levels as in the existing work, DEEF [7], is that in reality battery levels may fluctuate and the differences in battery levels across nodes may spur synchronization problems, which can cause packet drops. After deployment, sensor nodes traverse several functional states. The states mainly include node-stay alive, packet reception, transmission, encoding and decoding. As each of these actions occurs, the virtual energy in a sensor node is depleted. The current value of the virtual energy, Evc, in the node is used as the key to the key generation function, F. During the initial deployment, each sensor node will have the same Energy E_{ini}, therefore, the initial key, K_i, is a function of the initial virtual energy value and an Initialization Vector IV. The IVs are predistributed to the sensors. Subsequent keys K_j are a function of the current virtual energy, Evc, and the previous key Kprev. The exact procedure to compute virtual cost, Evc, slightly differs if a sensor node is the originator of the data or the forwarder. In order to successfully decode and\ authenticate a packet, a receiving node must keep track of the energy of the sending node to derive the key needed for decoding. In energy aware security scheme, the operation of tracking the energy of the sending node at the receiver is called watching and the energy value that is associated with the watched sensor is called Virtual Perceived Energy (Ep) as in [8].

```
Energy aware security scheme { Kprev, Evc} {
   Begin
        Ereq→size of data* Energy required to transmit unit data
        Eresidual → Eini-Eused
        If {Eresidual>=Ereq}
                Knew→Kprev *Eresidual
        Else
                Eneigh→ Neighbor node with highest energy
                If {Eneigh>=Ereq}
                        Forward sensed information through its neighbor
                        //Change the key for each and every packet
                        Knew→Kprev *Eresidual
        End
```

Crypto Module

Due to the resource constraints of WSNs, traditional digital signatures or encryption mechanisms requiring expensive cryptography is not viable. The scheme must be simple, yet effective. Thus, in this section, a simple encoding operation similar to that used in [9] was developed. The encoding operation is essentially the process of permutation of the bits in the packet, according to the dynamically created permutation code via the RSA encryption mechanism. The key to RSA is created by the previous module. The purpose of the crypto module is to provide simple confidentiality of the packet header and payload while ensuring the authenticity and integrity of sensed data without incurring transmission overhead of traditional schemes. However, since the key generation and handling process is done in another module, VEBEK's flexible architecture allows for adoption of stronger encryption mechanisms in lieu of encoding.

The packets in energy aware security scheme consist of the ID, type, and data fields. Each node sends these to its next hop. However, the sensors' ID, type, and the sensed data are transmitted in a pseudorandom fashion according to the result of RSA. More specifically, the RSA encryption algorithm takes the key and the packet fields as inputs and produces the result as a permutation code.

The concatenation of each 8-bit output becomes the resultant permutation code. As mentioned earlier, the key to the RSA mechanism is taken from the core virtual energy-based keying module, which is responsible for generating the dynamic key according to the residual virtual energy level. The resultant permutation code is used to encode the message. Then, an additional copy of the ID is also transmitted in the clear along with the encoded message. Thus, instead of the traditional approach of sending the hash value along with the information to be sent, the result of the permutation code value is used locally. When the next node along the path to the sink receives the packet, it generates the local permutation code to decode the packet.

System architecture

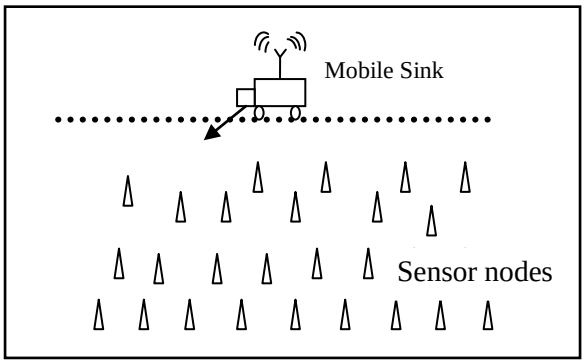

Figure.1 Three-Layer framework.

Figure.1 shows the architecture of the proposed system. The mobile sink sends data request messages to the sensor nodes directly. In the energy aware security scheme operational mode, nodes in the network are configured to only watch some of the nodes in the network. Each node randomly picks r nodes to monitor and stores the corresponding state before deployment. As a packet leaves the source node it passes through node that watch it probabilistically. Thus, Energy aware security scheme is a statistical filtering approach like SEF [10-12] and DEF [13]. If the current node is not watching the node that generated the packet, the packet is forwarded. If the node that generated the packet is being watched by the current node, the packet is decoded and the plaintext ID is compared with the decoded ID. If the watcher-forwarder node cannot find the key successfully, it will try as many keys as the value of virtual Key Search-Threshold before actually classifying the packet as malicious. If the packet is authentic, and this hop is not the final destination, the original packet is forwarded unless the node is currently bridging the network. In the bridging case, the original packet is re-encoded with the virtual bridge energy and forwarded. Since this node is bridging the network, both virtual and perceived energy values are decremented accordingly. If the packet is illegitimate, which is classified as such after exhausting all the virtual perceived energy values within the virtual Key Search Threshold window, the packet is discarded.

This process continues until the packet reaches the sink. This operational mode has more transmission overhead because packets from a malicious node may or may not be caught by a watcher node and they may reach the sink. However, it reduces the processing overhead.

The trade-off is that an illegitimate packet may traverse several hops before being dropped. The effectiveness of this scheme depends primarily on the value r, the number of nodes that each node watches.

Simulation Results

The proposed scheme is evaluated by using the NS-2 simulator. In the simulation, the radio nodes are connected in mesh topology. The initial energy set to each node is 20J. The transmission power is 0.7J. The node consumes 0.6J for receiving the data. There are 21 nodes distributed in the area 1000×1000.

Parameter	Value
Simulator	NS2
Simulation Time	20 ms
Number of nodes	21
Routing protocol	AODV
Traffic model	CBR
Simulation Area	1000×1000
Transmission range	250m

The networks parameters are recorded in the trace file during the execution of simulation. The performance of the network is analyzed by using the graphs. The graphs are executed in the trace file in NS2 simulator. Figure.3 gives the packet delivery ratio of Mobile sink. The graph is plotted between the No. of packets received and the simulation time. From the graph, the throughput of proposed scheme can be extracted as 180 packets per unit time. In this simulation the energy consumption by the mobile sink is analyzed by extracting the energy value from trace file. Figure.4 shows the graph for energy consumption. From the graph, the energy consumption of the proposed system is efficient than the existing techniques.

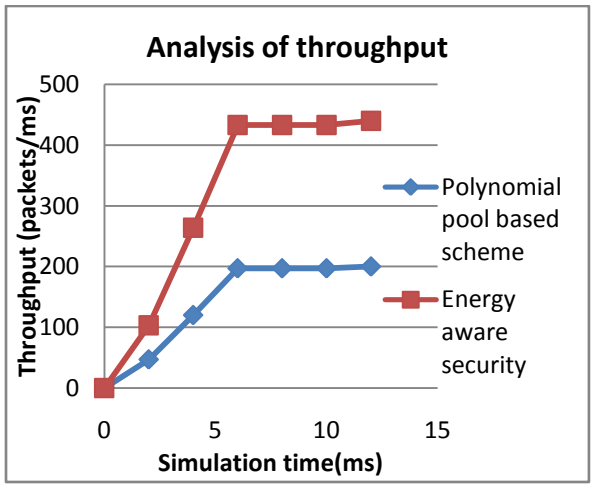

Figure.3 Throughput

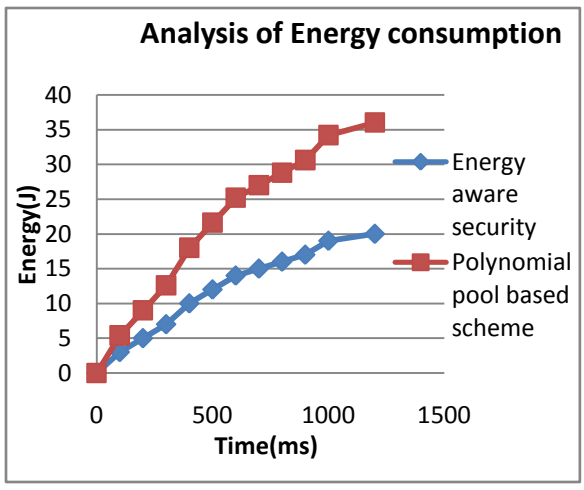

Figure.4 Energy consumption

Conclusion

In this paper, an energy aware security scheme is proposed for authentication and dynamic key establishment between mobile sinks and sensor nodes. The proposed scheme is based on energy aware dynamic key generation scheme and it has improved network resilience to replication attacks and the lifetime of the network. This proposed scheme provides the security with the awareness of residual energy of the sensors. The sensed information is encrypted by using the RSA algorithm.

The key generated by RSA algorithm is dynamically changed for each packet. The Energy based dynamic key generation algorithm is used to generate the dynamic key while the sensor node is in the demand to transmit the data packet. The mobile sink can aware of the residual energy of the sensors. So, based on the residual energy of the sensor, the mobile sink sends the data request. As the key is dynamically changed, the adversary cannot introduce replicated node in the network.

References

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, Mar. 2002.
2. C. Vu, R. Beyah, and Y. Li, "A Composite Event Detection in Wireless Sensor Networks," Proc. IEEE Int'l Performance, Computing, and Comm. Conf, Apr. 2007.1006 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010.
3. S. Uluagac, C. Lee, R. Beyah, and J. Copeland, "Designing Secure Protocols for Wireless Sensor Networks," Wireless Algorithms, Systems, and Applications, vol. 5258, pp. 503-514, Springer, 2008.
4. Crossbow Technology, http://www.xbow.com, 2008.
5. G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors," Comm. ACM, vol. 43, no. 5, pp. 51-58, 2000.
6. R. Roman, C. Alcaraz, and J. Lopez, "A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes," Mobile Networks and Applications, vol. 12, no. 4, pp. 231-244, Aug. 2007.
7. H. Hou, C. Corbett, Y. Li, and R. Beyah, "Dynamic Energy-Based Encoding and Filtering in Sensor Networks," Proc. IEEE Military Comm. Conf. (MILCOM '07), Oct. 2007.

8. L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security, pp. 41-4, 2002.
9. M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic Key Management in Sensor Networks," IEEE Comm. Magazine, vol. 44, no. 4, pp. 122-130, Apr. 2006.
10. M. Zorzi and R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Trans. Mobile Computing, vol. 2, no. 4, pp. 337-348, Oct.-Dec. 2003.
11. M. Vuran and I. Akyildiz, "Cross-Layer Analysis of Error Control in Wireless Sensor Networks," Proc. Third Ann. IEEE Comm. Soc. Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON '06), vol. 2, pp. 585-594, Sept. 2006.
12. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE J. Selected Areas in Comm., vol. 23, no. 4, pp. 839-850, Apr. 2005.
13. Z. Yu and Y. Guan, "A Dynamic En-Route Scheme for Filtering False Data Injection in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 1-12, Apr. 2006.