Secure and Energy Aware Mechanism in Wireless Sensor Network

[1] P. ThiruvannamalaiSivasankar, [2] Dr. M. Ramakrishnan

[1]Research Scholar, Sathyabama University, Chennai, India.

[2]School of Information Technology, Madurai Kamaraj University, India

Abstract

In Wireless sensor Network, providing security in a cost of efficient way is the major problem because of resource limited sensor devices. Therefore, we need to consider the energy of the sensor node while providing security. The wireless sensor network with mobile sink is vulnerable to replication attack. To avoid replication attack, the dynamic polynomial pool based key pre-distribution scheme is already present. But in that, the energy of the sensor node is not considered. Our proposed scheme provides security with the awareness of sensor node residual energy. The sensed information is encrypted 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 to generate the dynamic key while the sensor node is in the demand to transmit the data packet. The mobile sink aware of residual energy of sensors, therefore, based on the residual energy of the sensor, the marble sink sends a data request. As the key is dynamically changed, the adversary cannot introduce replicated node in the network.

Keyword :RSA;Residual energy;security;sink.

I. INTRODUCTION

Wireless sensor networks (WSN) can be used in a broad range of applications [1] and [2], such as military sensing, health monitoring, data acquisition, and habitat monitoring, etc. The data sensed by sensor node are frequently sent to the base station for analysis. In multi-hop communication security deteriorates since the distance between sensor nodes and base station is long (e.g., intermediate may modify sensor node's data by capturing, launching wormhole attack, Sybil attack, selective forwarding, sinkhole, etc.). Energy consumed by nodes close to base station increased and reduce the lifetime of the network. Therefore, mobile sink (MSs) is an important mechanism in the process of different wireless sensor networks (WSN) applications [4]. In the security aspects, the WSN is most important to give reliable, precise data to the adjacent nodes and to the base station. During this article, we spotlight on the process of keying method in this WSNs. The key management schemes for WSNs divided into two parts such as: static key management schemes and dynamic key management schemes.In static key schemes, key management functions such as key generation and distribution are statically handled. The static amount of keys loaded after deployment of the network in this static scheme of key management. The keying function performs periodically by the network in the dynamic key management schemes. The sensor nodes are exchanged the keys dynamically to communicate. The principle of this article is to extend secure and efficient communication framework for WSN applications. Particularly, in this article, we establish Energy based safe communication structure gives the method to validate data in order and fall fake packets from malevolent nodes. So, the potency of the sensor network is maintained. Energy aware security scheme dynamically updates keys exclusive of exchanging messages. An each sensed data is protected using an effortless encoding method and sent towards the base station. This method derived from a permutation code generated using the RSA (Rivest-Shamir-Adleman) encryption method. In this method the key is dynamically changing for the purpose of residual energy in the sensor node, therefore no need for re-keying. Consequently, one message generated using a single time dynamic key through the basis sensor node and dissimilar key used the stream of consecutive packets. The on warding data from sensor nodes beside the path to the base station are able to confirm the validity and the data reliability, to provide non refutation. We also illustrate that Energy aware security scheme is significantly more energy efficient than dynamic polynomial pool based key pre-distribution scheme.

II. PROPOSED SYSTEM

The energy-based keying part of the energy aware security scheme structure is the principal offerings this article and basically this process meant for managing the keying method It gives an active key feed intensively on the component of crypto. In this Energy aware security scheme, the sensor nodes form the initial deployed network and it has an assured essential value of energy. After deployment, sensor nodes pass through several useful states. The states generally consist of node-stay alive, communication, encoding, decoding, packet reception [11]. These of the actions occurs, the sensor node of the virtual energy is exhausted. E_{pv} is the present energy value. F is the function of key generation. E_{ini} is the energy level of the initial deployment, each sensor node and K1 are the initial key value of this function. The initialization of vectors is redistributed to the sensor nodes. Our proposed energy aware security scheme is described below.

The procedure to calculate virtual cost(Evc), slightly if an originator data of the sensor node. So, as to effectively decode the packet, a getting node should maintain path of on warding node energy to achieve the decoding based on the required key [12]. The energy aware security scheme, the process of the energy tracking by sending sensor node at the receiver, the related value of energy called Perceived Energy (Epe) as in [5] and [6].

```
Energy aware security scheme {Kprev, Evc} {
     Begin

             Energy-request   =   size of data* Energy required to transmit unit data

     Residual-Energy =  Eini -  E used  // some   initial  energy and E used  used   energy
             If (Residual-Energy    >=  Energy-E-request)
                     Knew = Kprev * Eresidual  // Kprev- privies key
             Else
                     Any =  Neighbor node with high energy
                     If {Eneigh >= Ereq}
                             Forward sensed information through its neighbor
                             //Change the key for each and every packet
                             Knew =  Kprev *  Eresidual
         End.
```

Fig 1: Energy aware security scheme

A. Crypto Module

In this Crypto Module, to establish an operation of encoding method and associated with [7]. In this method of operation is effective practice of the bits of permutation in the packet, based on the dynamically formed permutation code through the RSA encryption system. The key to RSA is created by the preceding module. The crypto module of the aim is simple confidentiality in the header of the packet and the payload of the packet whereas assuring integrity, authenticity of sensitive data with no acquiring communication transparency of conventional methods. In this energy aware security scheme the packet consists of l-bits ID and t-bits identifier of type, n-bits of data fields and these three fields are sent to subsequent hop. However, the ID of the sensors, type and sensed information transformed in a simulated random approach based on RSA type. The RSA encryption algorithm produces a permutation code as an outcome based on the inputs is the key and packet fields of the node. The consequential code of permutation is a combination of every eight bit output of encryption algorithm. The encode message is from the resultant permutation code and then transmitted in clear a replica of the ID along with encoded message. Thus, as an alternative of the conventional method of conveying the hash value (Message digests (MD) and Message Authentication Codes (MAC) are hash values) to be sent beside the information. The received packet information of the base station through the permutation code.

B. System Architectures

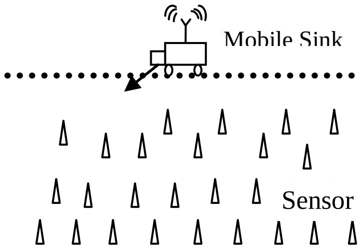

Fig 2 Three-Layer framework

Figure.2 shows the architecture of our proposed system. A mobile sink sends data request messages to the sensor nodes directly. Based on the operational mode in the energy aware security scheme, some of the observe sensor nodes are configured. Some of the sensor node picks randomly to monitor and stores the analogous state before deployment. The packet leaves from the originator node and passes through each sensor node. Thus, an Energy aware security scheme is a filtering of statistical technique like [8] and [9]. Suppose, the existing node is not inspecting node and produces the packet, that packet is on warded. If the packet produces from the sensor node is being watched by the present node and the packet is decoded, the decoded ID of the packet and ID of the plain text is comparing together. If the watcher-on warder node of the sensor cannot discover the key effectively, it will effort as various keys since the cost of a key search. The packet is classified as malicious If the packet of the sensor node is reliable, and hops not the ending destination; the new packet is forwarded except the sensor node is currently bridging the sensor network. The bridging case, the unique packet is decoded by virtual bridge energy and the packet is forwarded. Since this sensor node is bridging the sensor network, both perceived energy values (Epe) and virtual energy values are consequently decremented. If the node of the packet is illicit, it is categorized as such behind exhausting every one of virtual perceived energy values (Epe) in the effective Key Search Threshold window, the packet is redundant. This process continues until the node of the packet arrives the base station. This outfitted model has further transmission overhead since packets from a malicious node and reaches the sink. However, it decreases the processing transparency because decoding is not performed at every hop and less re-encoding is performed.

C. Simulation Results

The proposed scheme is evaluated by using the NS-2 simulator. In our simulation we are connecting the radio nodes in a 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. We have used two ray ground models for radio signal propagation. We have 21 nodes distributed in the area 1000×1000.The Results are obtained by executing our proposed protocol which is presented below.

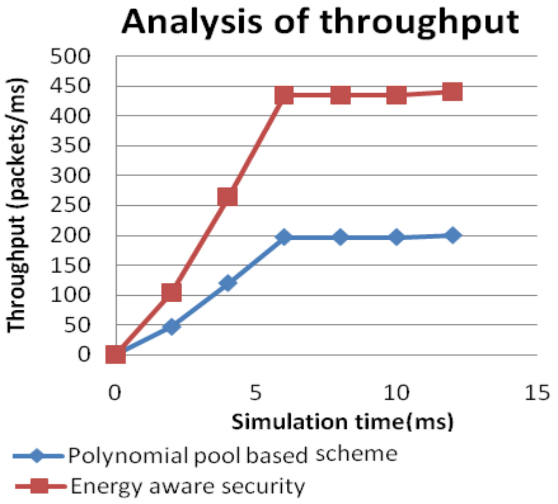

Fig. 3 Analysis of packet throughput

Table.1 Simulation result

	Value
Simulator	NS2(Ver. 2.28)
Simulation Time	20 ms
Number of nodes	21
Routing protocol	AODV
Traffic model	CBR
Simulation Area	1000×1000
Transmission range	250m

The network parameters are recorded in the trace file while the execution of the simulation. The performance of the network is analyzed by using the graphs. The graphs are getting by executing 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 we can extract the throughput of the proposed scheme as 180 packets per unit time.

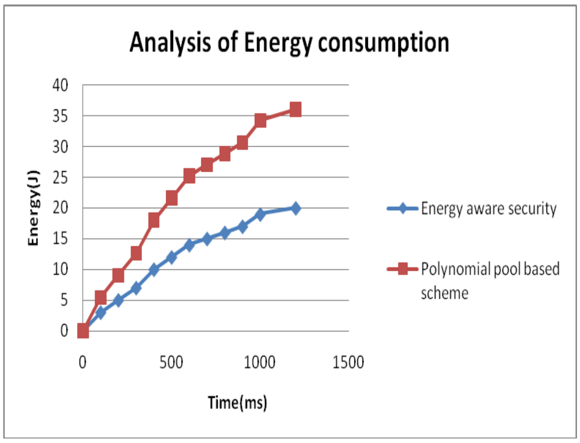

Fig.4 Analysis of energy consumption

In this simulation the energy consumption by the mobile sink is analyzed by extracting the energy value from the trace file. Figure.4 shows the graph for energy consumption of the proposed scheme. From the graph 3 and 4 , comparison based on the packet throughput and energy consumption of our proposed system is more efficient than the polynomial pool based scheme.

III. CONCLUSION

In this paper, we proposed an energy aware security scheme for authentication and dynamic key establishment between mobile sinks and sensor nodes. The projected method, based on energy aware dynamic key generation scheme considerably improved network resilience to replication attacks and improve the lifetime of the network. Our 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 is generated by RSA algorithm which is dynamically changed for each and every 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] K. Akkaya and M. Younis, “A Survey on Routing Protocols for Wireless Sensor Networks,” Ad Hoc Networks, vol. 3, pp. 325-349, May 2005.

[3] C. Vu, R. Beyah, and Y. Li, “A Composite Event Detection in Wireless Sensor Networks,” Proc. IEEE Int'l Performance, Computing, and Comm. Conf. (IPCCC ’07), Apr. 2007.1006 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010 Fig. 13. Synchronization ratio of nodes along the path to the sink.

[4] Rasheed, Amar, and Rabi N. Mahapatra. "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks", IEEE Transactions on Parallel and Distributed Systems, Issue No.05 - pp: 958-965 May (2012 Vol. 23).

[5] H. Hou, C. Corbett, Y. Li, and R. Bye, “Dynamic Energy-Based Encoding and Filtering in Sensor Networks,” Proc. IEEE Military Comm. Conf. (MILCOM ’07), Oct. 2007.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] He, Xiaobing, Michael Niedermeier, and Hermann de Meer. "Dynamic key management in wireless sensor networks: A survey", Journal of Network and Computer Applications, 2013.

[11] Vijay Anand, H. M., and G. Varaprasad."Dynamic key management method for wireless sensor networks", 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN),2012.

[12] Chythanya, K. Ravi. "Virtual Energy-Efficient Encryption and Keying (VEEEK) for Wireless Sensor Networks", International Journal of Computer Science & Engineering/09753397,2011080.