Volume 4, No. 7, July 2013

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

A SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS

Namdeep Singh[1], Er. Jasvir Singh[2]

[1]Dept. of Computer Engineering, University College of Engineering, Punjabi University, Patiala, Punjab, India
namdeepsingh@yahoo.com[1]
[2]Dept. of Computer Engineering, University College of Engineering, Punjabi University, Patiala, Punjab, India
jassiccet@gmail.com[2]

Abstract*:* Advancements in the technologies of micro electromechanical and embedded chips make it possible to design a tiny device with more powerful computations and communication features such as cryptography and wireless communication with low energy consumptions. Sensor devices are tiny in size and have limited resource (memory, energy, processing, low transmission range) such as MICA2DOT and T-Mote Sky. Traditional public key cryptographic techniques are not possible on these devices (such as RSA). To handle this problem ECC techniques have been developed for these small and limited resource devices. ECC consumes less energy and requires less memory and bandwidth than RSA with same level of security. Public key cryptographic techniques provide more security as compare to symmetric key cryptographic techniques at the cost of more energy consumption and more resource utilization. So, for balancing energy consumption and security level the Hybrid cryptographic techniques have been developed for Wireless Sensor Networks (WSNs). By using Hybrid cryptographic techniques few security frameworks have been proposed in past few years to provide more security and with less memory requirements. This paper provides an overview of some common WSNs concepts and proposed a security framework for LEACH protocols.

Keywords: MICA2DOT, LEACH, Security Framework, T-Mote Sky, WSNs

INTRODUCTION

WSNs are network of sensor nodes which communicate with each other’s and to the base station using wireless channel. These sensor nodes sense the physical world phenomena’s and by converted it to digital data send to the base station for analysis, storage, processing, mining. Sensor nodes communicate to base station by single-hop or by multi-hop. In single-hop sensor data directly to the base station and in multi-hop sensor data is send to intermediate node or data aggregate node which aggregate data coming from sensor nodes, then send to the base station. For communication in WSNs many routing protocols were developed by the researchers. All major routing protocols are divided into seven categories [1]. These categories are

1. Location-based Protocols
2. Data Centric Protocols
3. Hierarchical Protocols
4. Mobility-based Protocols
5. Multipath-based Protocols
6. Heterogeneity-based Protocols
7. QoS-based Protocols

From these categories Hierarchical Protocols are an energy-efficient communication protocols such as Low-Energy adaptive Clustering Hierarchy protocol [2] which is the most popular energy-efficient hierarchical clustering algorithm proposed for reducing power consumption. This protocol does not provide any security itself. So, different security frameworks were proposed for these types of protocols.

The rest of the paper is organized as section 2 provides related work, section 3 overviews security goals , section 4 provides proposed work, section 5 provides experiment results and section 6 present the conclusion

RELATED WORK

Suraj Sharma et al. provides a survey on secure hierarchical routing protocols in WSNs in [3], in which they compare M. Bohge et al, SRPSN, LHA-SP, F-LEACH, SLEACH, SHEER, R. Srinath et al., NHRPA, Sec-LEACH, SS-LEACH, RLEACH, ESMR, SRPBCG protocols. They also provide overview of these protocols that are as follows:

M. Bohge et al. [4] proposed a secure hierarchical protocol by using three-tier ad-hoc network topology. For authentication it used a TESLA certificate and the framework protest all data against malicious modification and information forgery by using message authentication code. It presented an application driven hierarchical ad-hoc sensor network authentication framework which deals with compromised nodes. But it cannot prevent network from intruders and sending packets and cannot provide protect from eavesdropping.

In SRPSN [5], author proposed an energy-efficient level-based hierarchical routing technique. They have design a secure routing protocol for WSNs to protect from different attacks by making a secure route from source to sink. In this symmetric key cryptography technique is used and a group key management scheme is proposed, which contains group communication policies, group membership requirements and an algorithm for generating a distributed group key for secure communication. Every node is contributing in its partial key to generate a group key. A drawback of this protocol is that, while changing the CH (Cluster Head) all group key i.e. inter-cluster and intra-cluster key should have to compute once again, which is a cumbersome task.

LHA-SP [6] is focusing on securing heterogeneous hierarchical WSNs with arbitrary number of levels. The symmetric key scheme is used in it and took following assumption: an advisory will take a certain amount of time to compromise the group key or temper with a node and this amount of time exceeds, that require setup the network. It protects from intruders to taking activity, tempering with or injecting message into the networks and also protects from eavesdropping on communication between legitimate nodes. Shared pair-wise key is used to maintain authentication and confidentiality. It deals with orphan node problem.

F-LEACH [7] is a protocol proposed by L, B. Oliveria et al. for securing node to node communication in LEACH-based network. For enhancing security in LEACH, random key pre-distribution scheme with symmetric key cryptography is used. It provides authentication, integrity, confidentiality and freshness to node-to-node communication. But it cannot protect from node capturing attack.

SLEACH [8] is the first modified secure version of LEACH, which investigated the problem of adding security to cluster-based communication protocol for homogeneous WSNs consisting of nodes with several limited resources. It uses building blocks of SPINS (Security Protocol for Sensor Network), symmetric key methods, and MAC (Message Authentication code) for securing LEACH. It provides protection from selective forwarding, sinkhole and HELLO flooding attacks. It also protect from intruders to send bogus sensor data to the CH and CH to forward bogus message. But it cannot prevent to crowd the time slot schedule of a cluster, which causes DoS attack or simply lowering the throughput of the CH and does not guarantee of data confidentiality. It meant for protect from outside attacks.

SHEER [9] is proposed by J. Ibriq et al. it is a Secure Hierarchical Energy-Efficient Routing protocol which provides secure communication at network layer. The probability broadcast mechanism and three-level hierarchical clustering architecture is used to improve the energy performance and increase lifetime. It implements HIKES a secure key transmission protocol and symmetric key cryptography to secure the routing. They have compared the performance with secure LEACH using HIKES.

R. Srinath et al. proposed an Authentication Confidentiality cluster based secure routing protocol [10], which is based on LEACH protocol. Public key (in digital signature) and private key cryptography both are used in it. It deals with interior adversary or compromised node. Due to high computation requirement of public key cryptography it is not efficient in WSNs.

NHRPA [11] is routing protocol which adopts suitable routing technology for the nodes according to the distance of node to Base Station, density of the nodes distributed and residual energy of the nodes. It compared with Directed Diffusion (DD), LEACH, and PEGASIS in terms of the energy usage, packet latency and security in the presence of node compromised attacks, the proposed routing algorithm results show that it is more efficient for WSNs. This routing protocol does not use any cryptography technique, so the overhead is less. But only node compromise attack is prevented in it.

Sec-LEACH [12] provides an efficient solution for securing communication in LEACH. Random-key pre-distribution and µTESLA is used in it for secure hierarchical cluster heads and dynamic cluster formation. Random-key distribution is applied in Sec-LEACH and symmetric key and one way hash chain is introduced to provide confidentiality and freshness. It provides authenticity, integrity, confidentiality and freshness to communication.

SS-LEACH [13] proposed by Di Wu et al. which is a secure hierarchical protocol. It is the secure version of LEACH. In this the method of electing cluster heads is improved and forms dynamic stochastic multi-paths cluster heads chains to communicate to the base station. By this way it improve the energy efficiency and prolong the network lifetime. The key pre-distribution and self-localization technique is used to secure the basic LEACH protocol. It protects the network from compromised node to take a part and preserve the secrecy of the packet. Selective forwarding, HELLO flooding and Sybil attacks are avoided in it.

RLEACH [14] is a secure solution for LEACH in which cluster are formed dynamically and periodically. The orphan node problem is raised in RLEACH due to random pair-wise key scheme so they used improve random pair-wise key scheme to overcome it. The one way hash chain, symmetric and asymmetric cryptography has been used in RLEACH to provide security in LEACH. To many attacks are resists in RLEACH like spoofed, alter, and replayed information, sinkhole, wormhole, selective forwarding, HELLO flooding and Sybil attack.

ESMR [15] is an efficient security model of routing protocol to provide the security solution for the LEACH; only public key cryptography technique is used in it. The performance of ESMR by simulation results show that is not good as LEACH when there is no attacker in network, but as the number of attacker increases it becomes better and better. Out-sider attacks are only prevented in this protocol and it has high computation burden due to the use of public key cryptography.

SRPBCG [16] proposed by Z. Quan et al. is a secure routing protocol cluster-gene-based for WSNs. The selection of cluster head is same as LEACH. The objective of this scheme is to manage trust and reputation locally and to authenticate identity of node with minimal overhead and time delay. It uses biological authentication mechanism which is a very effective authentication method, using biological 'gene' as encryption key is very secure and effective key distribution scheme, which requires only few memory and communication overhead. This protocol only deals with adversary's attack and compromised nodes. Security of this protocol is inconsiderably, when forms cluster and transmitting the message. In this protocol computation and communication burden is more.

SECURITY GOALS IN WSN

Security goal [3] of any network is to provide security services to defend against all the kinds of threats. These services include the following:

Confidentiality

Confidentiality is to protect data during communication in a network to be understood other then intended recipient. Cryptography techniques are used to provide confidentiality.

Integrity

Integrity ensures that the data should not be altering during its transmission. The techniques like message digest and MAC are applied to maintain integrity of the data.

Authenticity

Authenticity allows the receiver to verify that the message is sent by authorized user. Cryptography mechanism like MAC can be maintaining authenticity.

Availability

Availability ensures that the services are always available in the network even under the attack such as Denial of Service attack (Dos). The researchers proposed different mechanisms to achieve this goal.

Freshness

Freshness ensures that the data received by the receiver is the recent and fresh data and no adversary can replay the old data. The freshness is achieved by using mechanisms like nonce or timestamp should add to each data packet.

PROPOSED WORK

In this paper a security framework based on ECC and AES cryptography system is proposed. In this work solar-aware distributed LEACH protocol [17] is used without any change in its algorithm as proposed by the author. We only applied spoofing attack on it in OMNet++ simulator and then applied our proposed framework to check performance, the energy consumption used for cryptography techniques are taken for ECC is from TinyECC [18] [19], and for AES is from [20].

Solar-aware distributed LEACH

Solar-aware distributed LEACH protocol is work in rounds like original distributed LEACH. And in each round two phases are used one for electing cluster heads i.e. set-up phase and other for data transferring i.e. steady-phase. Each round has only single set-up phase and multiple steady-phases as show in figure 1 [17].

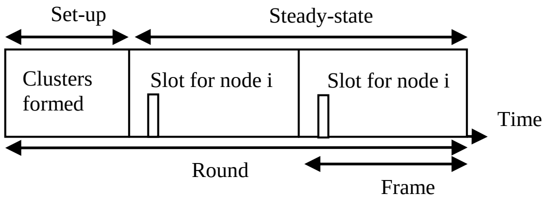

Figure 1. LEACH operations

In solar-aware distributed LEACH set-up phase takes three steps and steady-state phase takes two steps as follows-

Set-up phase

1. N_i → BS : ID_{Ni} , ID_{BS}, E_{Ni}, Pos_{Ni}
2. BS ⇒ N_i : ID_{BS}, ID_{Ni}, ID_{CH}
3. CH ⇒ C : $ID_{CH,}$ ID_{c}, T_{C}

Steady-state phase

4. C → CH : ID_{C}, ID_{CH}, D_{C}
5. CH → BS : ID_{CH}, ID_{BS}, F(D c)

The various symbols denotes:

N_i, CH, BS	A sensor node, cluster head and base station
E_{Ni}	: Energy of i^{th} node
Pos_{Ni}	: Position of i^{th} node
→	: Unicast
⇒	: Broadcast
C	: cluster or group of nodes in cluster
T_{c}	: Time slot for nodes in a cluster
F	: function for data aggregation
D_{c}	: Data of nodes in cluster

During set-up phase sensor nodes send their energy and position to the base station for electing cluster heads and base station applied cluster head selection algorithm to electing nodes for becoming cluster head and by using broadcast, announces cluster heads and sensor nodes for each cluster head to the sensor nodes in the network. The elected cluster heads makes TDMA (time division multiple access) slots for their sensor nodes which comes under its cluster and sends these TDMA slots to cluster nodes for sending data to it in given slot.

After set-up phase steady-state phase starts in which sensor nodes send their data to their allotted cluster head and cluster head aggregate this data coming from all its sensor nodes and send to base station. After some pre-defined number of steady-state phase the next round will be started.

Adding Security to Solar-aware LEACH

Our proposed security framework for solar-aware distributed LEACH is as follows-

Set-up phase

1. N_i → BS :ID_{Ni} , ID_{BS}, Enc_{S} (ID_{Ni}| E_{Ni}| Pos_{Ni})

   BS : if Dec_{S} (ID_{Ni}| E_{Ni}| Pos_{Ni})

   Gen. : new S_{k}
2. BS ⇒ N_i : ID_{BS}, ID_{Ni}, Enc_{P} (ID_{CH}| S_{k})

   N_i :if Dec_{p} (ID_{CH}| S_{k})

   Set : new S_k
3. CH ⇒ C : $ID_{CH,}$ ID_{c}, Enc_{Sk} (ID_{C}| T_{C})

   C : if Dec_{Sk}(ID_C| T_C)

Steady-state phase

4. C → CH : ID_{C}, ID_{CH}, Enc_{Sk} (D_{C})
5. CH → BS : ID_{CH}, ID_{BS}, F(Enc_{Sk} (D c))

Following additions with the previously defined symbols

Enc_{S} : Encryption using master symmetric key

Dec$_{S}$	: Decryption using master symmetric key
S$_{K}$	: new symmetric keys (one for each cluster)
Enc$_{P}$	: encryption using public key of nodes
Dec$_{P}$	: decryption using private key of node
Enc$_{Sk}$	: Encryption using new symmetric key
Dec$_{Sk}$	: Decryption using new symmetric key
Gen.	: Generate new key

In our work we use pre-distrusted key technique and hybrid cryptography technique. The keys are generated by the base station for every sensor node and distributed before developing in the network. These keys are asymmetric key for every sensor node and a common symmetric master key. The asymmetric key have public key of each node which is used by the base station for encrypting messages for sensor nodes and their corresponding private keys are used by the sensor node for decrypting their messages received from base station.

During initialization the master symmetric key is used for encrypting information and send to the base station. Then base station use same symmetric key for decrypting the message and apply algorithm for electing cluster heads. When cluster heads are elected, then base station generates new symmetric keys equal to the number of cluster heads.

Then base station encrypts the message using sensor nodes public keys and broadcast message to the network. Now, in this case new generated keys are added in message for changing master symmetric key this will increase the size of the original announcement message, which depends on the size of symmetric key.

Then sensor nodes receive message from base station and decrypt it using their private key and set their cluster heads and change their master key with new key. Now, this new key is used in the steady-state phase for encryption and decryption and the master key is change dynamically during each set-up phase by base station. And for allotting TDMA cluster heads and sensor nodes uses their new master key.

In steady-state phase data is encrypted using new master key by sensor nodes and send to cluster head. The cluster heads only aggregate their received messages and send to base station. The cluster heads does not need to decrypt data they only check that the data received is only send by correct node in their given TDMA slot.

The integrity of data is only checked by the base station. There is need to store only two keys per node one private key and other is symmetric key, which save memory requirement and Base station have public keys of each node and symmetric keys are equal to the number of clusters, all key generation and distribution work is done at the base station only, which save key generation energy consumption at sensor nodes.

EXPIREMENT RESULTS

We implement the same solar-aware distributed LEACH given by [17]. We have only applied attack on it and the results without attack and with attack are show in figure 2 and figure 3, respectively. Figure 4 show the result of proposed security framework.

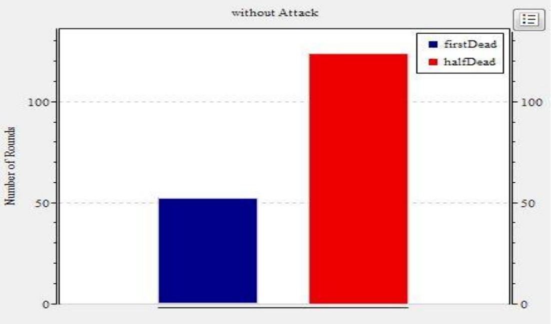

Figure 2. without attack

Figure 2 shows that the first is dead after 52 rounds and half of the nodes are after 124 rounds when there is no attack is present in the network.

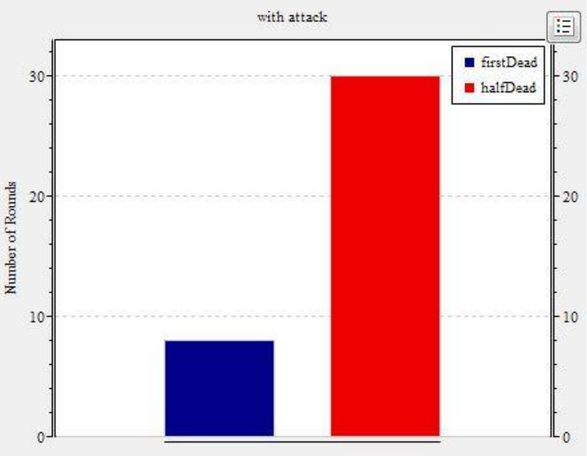

Figure 3. with Attack present in the network

When an attack is present in the network the performance of the network becomes degraded as shown in the figure 3. Figure 3 shows that first node is dead after 8 rounds only as compare to without attack results the performance is degraded 44 % for first in the presence of only single attack and half of the nodes are dead after 124 rounds when there is no attack is present, but when attack is present it takes only 30 rounds in this case 94 % performance is degraded.

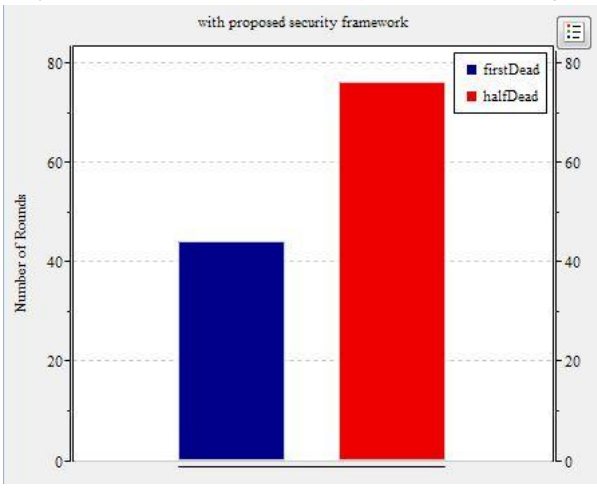

Figure 4. with proposed security framework

The performance of proposed framework is shown in Figure 4. It performs better, when there is an attack present in the network, but not as good as the network without it in the absence of the attack. As the number of attack increase its performance is better. After implementing security framework the first node takes 44 rounds and half of the nodes take 76 rounds to be dead.

CONCLUSION

In this a security framework is proposed for hierarchical routing protocols of WSNs, which uses Hybrid cryptography technique for encryption and decryption of messages for secure communication. The ECC encryption and decryption is used only for announcing cluster heads and distribute the symmetric keys during set-up phase. Nodes only decrypt the base station messages by using their pre-distributed private key. This framework is checked in solar-aware distributed LEACH protocol which is the improved version of LEACH protocol. This framework shows good results when attacks on routing is present in the network. But, due to cryptography techniques is not perform well as the network without attack. This framework protects the network from Spoofing, alter and replying information attack, Selective forwarding attack, Sybil attack, Hello flooding attack.

REFERENCES

[1] Shio Kumar Singh, M P Singh, and D K Singh, “Routing Protocols in Wireless Sensor Networks- A Survey”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol. 1, No.2, November 2010.

[2] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”, International Conference on System Sciences, Hawaii, January, 2000.

[3] Suraj Sharma and Sanjay Kumar Jena, “A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks”, ICCCS, Rourkela, Odisha, India, February, 2011.

[4] M. Bohge and W. Trappe, “An authentication framework for hierarchical ad hoc sensor networks”, in Proceedings of the 2nd ACM workshop on Wireless Security (WiSe’03), pages 79- 87, New York, NY, USA, 2003, ACM.

[5] M. Tubaishat, J. Yin, B. Panja, and S. Madria, “A Secure Hierarchical Model for Sensor Network”, ACM SIGMOD Record, 33(1):7-13, March 2004.

[6] B. Parno, M. Luk, E.Gaustad, and A. Perrig, “Lha-sp: secure protocols for hierarchical wireless sensor networks”, In Proceedings of 9th IFIP/IEEE International Symposium on Integrated Network Management, pages 33-44, May 2005.

[7] L. B. Olivera, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, “Secleach- a random key distribution solution for securing clustered sensor networks”, In Proceeding of the 5th IEEE International Symposium on Network Computing and Applications, pages 145-154, Washington, DC, USA, 2006, IEEE Computer Society.

[8] A. C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro, “On the security of cluster-based communication protocols for wireless sensor networks”, In Proceeding of 4th IEEE International Conference on Networking (ICNS05),volume 3420 of lecture Notes in Computer Science, pages 449-458, 2005.

[9] J. Ibriq, and I. Mahgoub, “A secure hierarchical routing protocol for wireless sensor networks”, In Proceedings of 10th IEEE International Conference on Communication Systems, pages 1-6, Singapore, October 2006.

[10] R. Srinath, A. V. Reddy, and R. Srinivasan, “Ac: cluster based secure routing protocol for wsn”, In Proceedings of the 3rd International Conference on Networking and Services, page 45, Washington, DC, USA, 2007, IEEE Computer Society.

[11] C. Hong-bing, Y. Geng, and H. Su-jun, “NHRPA: a novel hierarchical routing protocol algorithm for wireless sensor networks”, The Journal of China Universities of Posts and Telecommunications, 15(3):75-81, September 2008.

[12] L. B. Oliveira, A. Ferreira, M. A. Vilaca, H.C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, “Secleach- on the security of clustered sensor networks”, Signal Processing, 87(12):2882-2895, December 2007.

[13] D. Wu, G. Ni, “Research and improve on secure routing protocols in wireless sensor networks”, In 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008), pages 853-856, May 2008.

[14] K. Zhang, C. Wang, and C. Wang, “A secure routing protocol for cluster-based wireless sensor networks using group key management”, In Proceedings of the 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM’08), pages 1-5, October 2008.

[15] J. Chen, H. Zhang, and J. Hu, “An efficiency security model of routing protocol in wireless sensor networks”, In Proceedings of the 2nd Asia International Conference on Modeling and Simulation, 2008, pages 59-64, Washington, DC, USA, 2008, IEEE Computer Society.

[16] Z. Quan and J. Li., “Secure routing protocol cluster-gene-based for wireless sensor networks”, In Proceedings of the 1st International Conference on Information Science and Engineering (ICISE 2009), pages 4098-4102, December 2009.

[17] T. Voigt, A. Dunkels, J. Alonso, H. Ritter and J. Schiller, “Solar-aware Clustering in Wireless Sensor Networks”, In Proceedings of the 9th International Symposium on Computers and Communications, 2004, (ISCC 2004), Volume 1, pages 238-243.

[18] A. Liu, P. Ning, “TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wirless Sensor Networks”, International Conference on Information Processing in Sensor Networks, 2008 (IPSN08), pages 245-256.

[19] A. S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz, “Energy analysis of Public-key cryptography for Wireless Sensor Networks”, In Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications, 2005 (PerCom 2005), pages 324-328.

[20] T. Chung and U. Roedig, “On the feasibility of a new defense layer for wireless sensor networks using RF ranging”, In International Conference on Network and Service Security, 2009 (N2S’09), pages 1-6.