Key Management for Wireless Sensor Network Security

Gaith A. Muslim
Dept. of Computer Science
College of Computer Science and Information Technology
Basra University, Iraq

Ra'ad A. Muhajjar, PhD
Dept. of Computer Science
College of Computer Science and Information Technology
Basra University, Iraq

ABSTRACT
Most applications use wireless sensor networks (WSNs) to collect data, which are considered low-cost solutions to a variety of real-world problems. Sensors are small gadget that performs a certain function when deployed in the goal environment.

Due to the nature of the channel transport wireless and limited the resource of sensors. Security issues have become a critical challenge in WSNs. The information is critical so securing it is property cannot be dispensed in wireless sensor networks.

In this paper, security schemes have been proposed for securing hierarchical WSNs. The proposed scheme used a lightweight symmetric cryptographic technique that depends on a BLOOM hierarchal scheme and Pseudo-Random Number Generator (PRNG) to establish keys. The suggested method has a high level of security and makes efficient use of sensor resources.

Keywords
Wireless Sensor Network (WSN), Hierarchical wireless sensor networks, cluster-head (CH), security, Leach Protocol, key management, pseudo-random number generator (PRNG), rivets cipher (RC5)

1. INTRODUCTION
Wireless sensor networks are made up of a large number of sensors (They are tiny in size and have bounded sources) after deployed in the required environment to do certain missions such as temperature, pressure, humidity etc. based on the application that will be used. These sensors can communicate with each other by wireless channels, to send the sensed data from the surrounding area to the sink to treat it through single-hop if the sink is in the same range as the sender node or via multi-hops (node after node to the sink) if the sink is far away from the range of the sender node [1].

Where wireless sensor networks have received much interest for using it in a variety of applications, including military, environmental monitoring, and industrial [2]. All sensor nodes which consist it the wireless sensor networks are bounded of whence processing, connectivity, and power. As a result, one must consider this at designinga WSN. Asymmetric cryptographic algorithms are not suitable for building a safety system for a WSN due it requires high cost [3].

Sensor nodes in WSN are typically split into clusters small. A cluster is a collection of sensor nodes, with one node serving as the cluster head. Any cluster would have a cluster head who would be in charge of gathering sensing data from the cluster's members, with the rest nodes serving as member nodes [4].

Clustering in wireless sensor networks decreases the amount of exchanged connection, resulting in reduced battery consumption of individual sensor nodes. This extends the wireless sensor network's life span. For each cluster, a cluster-head is determined depending on the node's energy scale or distance. The basic goal is to connect the cluster-head only with the sink, leaving the remaining node in a condition of rest. A cluster-based wireless sensor network can be executed in both homogeneous and heterogeneous wireless sensor networks [5].

2. RELATED WORK
Key management in wireless sensor networks is a fundamental problem that has been addressed in a number of studies.

Lein Harn, et.al. A hierarchical key management and distribution strategy is proposed in this study. Key distribution system assures existed pair-wise key connect any node in the group with other nodes, and node with cluster head, each cluster head with the base station. The system also includes a security feature that demonstrates its resistance to sensor capture assaults. Lastly, the scheme necessitates sensor nodes with low memory, connection, and compute requirements [6].

Djamila Djibril, This research offered certain security goals for Wireless Sensor Networks, As well as various security strategies to combat these threats. Because of the importance of security in the acceptability and use of sensor networks for a variety of applications. Some protocols have advantages and disadvantages, while some security protocols have vulnerabilities. The main goal of this paper is to provide in-depth information regarding security challenges and methods of attacks on WSN, as well as some potential countermeasures [7].

Dr. Jidong Wang, et.al. Proposed a secure efficient, and easy-to-use hierarchical key management system, that is described in their study. The method allows three different types of keys to be created to encrypt communications transferred between sensor nodes which are group key, network key, and pairwise key.Must encrypt broadcast messages and validate modern nodes by network key. The group key shares the nodes inside the cluster. A pairwise key is a key that is shared between two nodes. Key generated, key transport, methods following sensor node running, and dynamical mellowness of keys are all covered by SHEKM.SEHKM is particularly efficient in computing and communication, according to the performance study and simulation [8].

P. Raghu Vamsi and Krishna Kant, The authors of this research examined multiple key management techniques created for WSNs, as well as their taxonomy in relation to several network and security parameters. In this essay, the authors explore important management ideas in order to create key agreement protocols and assessment metrics.

An analysis of recent advancements in KM has been presented in conjunction with these notions. In the case of network dynamics, dynamic KM, network heterogeneity, and mobility, it is noticed that important agreement design criteria such as scalability, resistance, revocation, and resiliency requires deeper exploration [9].

3. THE PROPOSED METHOD

Building and implementing an efficient security system for a WSN is our goal, done enhancing the existing key management by a safety system that takes into account the sensors' bounded resources and conserves them for as tall as possible. Each connected party must have a secure to safeguard the data that is exchanged in the WSN. Therefore, there must be a common key between each end of the communication in order to implement cryptography and meet security standards.

3.1 Key Generate

Before deploying the sensor nodes in the goal environment, each sensor is pre-loaded with an initial key and a unique identification. Clustering is done using the leach protocol after the deployment step to secure WSN. However, a key must be generated between each connected two-node.

In our proposed method, the key between the cluster-heads and the sink established bythe bloom scheme isan efficient way to preservethe sensor resource while the key between the cluster-heads and the respective member nodes is generated using the proposed pseudo-random number generator (PRNG).

3.1.1 Key Generate (CH-Sink)

The traditional bloom technique that is employed in hierarchical networks provides adequate security and needs large connection and calculation. As a result, in our proposed protocol we applied the bloom scheme in an effective manner to address the existing faults. To begin, the sink creates a public matrix G x+1*n through a limited range GF (q), with the only restriction that columns be linearly independent. We selected a non-binary Hadamard matrix in our proposed method since it has the least computing complexity, where q is the smallest prime integer greater than the number of sensor nodes.

G_{t+1*n}	1	1	1	1	.	.	.	n
	1	1	1	-1 mod q	.	.	.	.
	1	1	-1 mod q	-1 mod q	.	.	.	.
	1	-1 mod q	-1 mod q	1	.	.	.	.
	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.
	t + 1	.	.	.	.	.	.	.

Subsequently, over the finite field GF (q) the symmetric matrix S must be created at random.

$S_{t+1*t+1}$ =	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	.	.	.	$S_{1,t+1}$
	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$	.	.	.	$S_{2,t+1}$
	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$	.	.	.	$S_{3,t+1}$
	.	.	.	.	.	.	.
	.	.	.	.	.	.	.
	.	.	.	.	.	.	.
	$S_{t+1,1}$	$S_{t+1,2}$	$S_{t+1,3}$	.	.	.	$S_{t+1,t+1}$

Pummeled each from matrix S in P to compute matrix A then reverse matrix it.

$$A=[S*P]^T$$

Each row of the A matrix is encrypted by the initial key to cluster- head then sends the row encrypted to the goal cluster-head with the ch-id, which represents the sequence of the rows.

Rivets cipher5(RC5) method that is used to encrypt rows (message) received by cluster-head. After that, the cluster head will decrypt the received message and store it in memory space. Cluster-head will decrypt the received message and store it in memory space. All cluster head now has row and ch_id. After that must generation key between BS-CH in the second stage.

The connection is directly between the sink and cluster heads through one hop. Hadamard matrix approach is used to construct the matching public column on ch_id and the shared key is obtained as follows:

SH_key sn (i) = row sn(i) * public col. sn(j).
SH_key sn (j) = row sn(j) * public col. sn(i).

3.1.2 Key Generate (BS - SN)

The sink and sensors both have an initial key that was pre-loaded before the sensors nodes distribution.

The sink will begin generating the shared key and authentication key, which are derived from the shared key with sensing nodes by initial key and (pseudo-random number generator).

Using the initial key, the sink encrypts the shared key and the authentication key to send both to the respective cluster-head using the BS-CH key. Turn, cluster-head sends them to the member nodes.

Algorithm of Pseud-Random Number Generator

Step1)
- Input the initial key and use java securitymessage digest (md5) to create the hash.
- The initial key has been split into four partsp1, p2, p3, p4.

A) For j from 1 to 32

- Z ← [bit xor (p1 , p4)].
- Y ← [bit xor (p2 , p3)].

- For u from 1 to 32
- V ← [swapping (Y) <<>>5].
- End

- X ← addition (Z , V) module 2^32.
- T ← [bit xor (Z , Y)].
- Q ← [bit xor (V , X)].

- For l from 1 to 32
- U ← [swapping (Q)<<>>9].
- End

- F ← addition (T, U) module 2^32.
- a1 ← [bit xor (X , U)].

- **End**

B) For j from 1 to 32
- For s from 1 to 32
- b1 ← [bit xor (V)].
- End

C)
- c1 ← [bit xor (V , F)].

D)

- For n from 1 to 32
- d1 ← [bit not (F)].
- End

- **End**

- **A** ← [binary Vector to Hex (a1)].
- **B** ← [binary Vector to Hex (b1)].
- **C** ← [binary Vector to Hex (c1)].
- **D** ← [binary Vector to Hex (d1)].

Step2)

- Final key ← strcat [**A** , **B** , **C** , **D**] shared key (128 bit) is a combination of the four registers.

3.1.3 Key-Updating

The key must refresh frequently after a specific amount of time to prevent the attacker from gaining access to the current key information. In the suggested protocol, the shared key between the nodes in WSN must be changed; therefore, the sink sends a new row encrypted by the initial key to the cluster-head and then repeats the step (3.1.1).

The shared key between BS-SN must be updated, which is accomplished by feeding the old shared key BS-SN into the PRNG, which generates two keys, one of which is the new shared key between BS-SN and the other is the new Auth_key. As explained in paragraph (3.1.2).

3.1.4 Node Addition and Deletion

The new sensor might be stated as a cluster head or as a member node to an existing cluster head. In case becomes the additional node the cluster head, it sends a request letter to the sink, to which the sink responds with the new sensor's row and identity the cluster-head (ch_id). It will then generate a shared key, as described in the key generation phase (3.1.1).

In case becomes the additional node is a member node of the cluster head, the cluster head sends a row to the sink to authenticate the new node and obtain the new member's initial key, after which the shared key is generated as previously mentioned. If any nodes fail or are compromised, the sink sends a message to each node in the network, instructing them to erase the node's id from the nodes' adjacent tables.

4. ENCRYPTION AND DECRYPTION TECHNIQUE

For the sake of providing high security, the security requirements (confidentiality, integrity, and authentication) must be met. In this paper, the RC5 is employed to do this task which prevents the antagonist from realizing the messages [10].

Where every sensor has a unique (encryption/decryption) shared key as well as a unique authentication key. The key employed in our suggested approaches had a length of 128 bits.

5. STANDARD STATISTICAL TESTS

Cryptosystems use keys that must be produced at random. So, many cryptographic systems require Random Number (RN) or Pseudo-Random Number Generators (PRNG) as inputs. There are many of tested that must proceed according to the (NIST) as follows [11]:

Frequency test, Serial test, Runs test, Linear Complexity test, approximate entropy test.

6. PERFORMANCE EVALUATION

Figure (1) displays the distribution of 100 nodes in a100m*100m area wherethe sink position

(50,95) and sensor resources are limited (0.5 J of Energy, forty of range, low computational capacity).

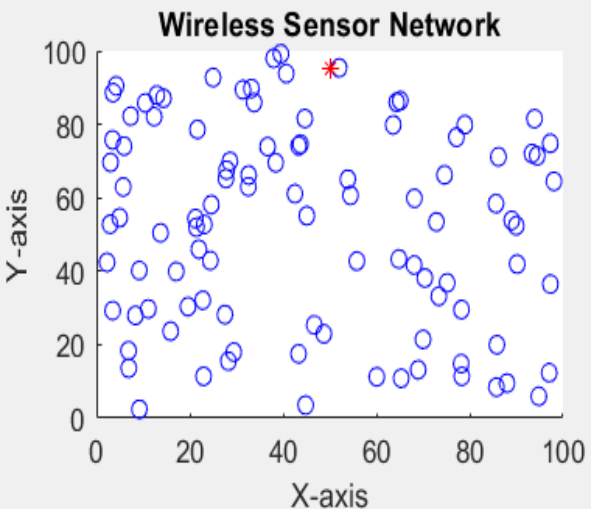

Figure (1) Random Deployment Of sensor Nodes.

Figure (2) displays the outcome of the clustering step utilizing the leach approach.

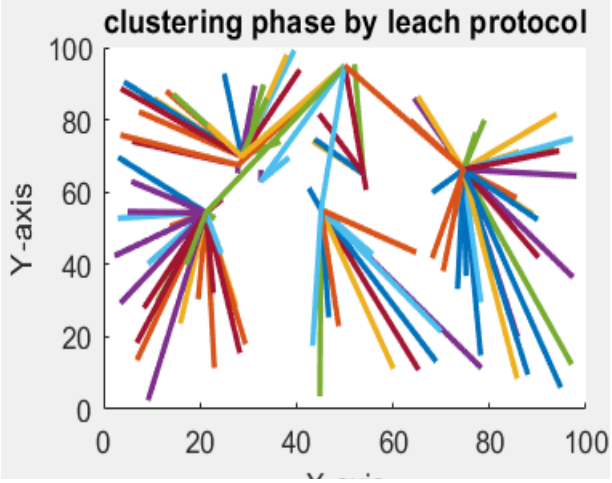

Figure (2)Clustering stage

Figure (3) compares the energy consumed for establishing shared keys. The energy consumption in our suggested method is lower than the previous method.

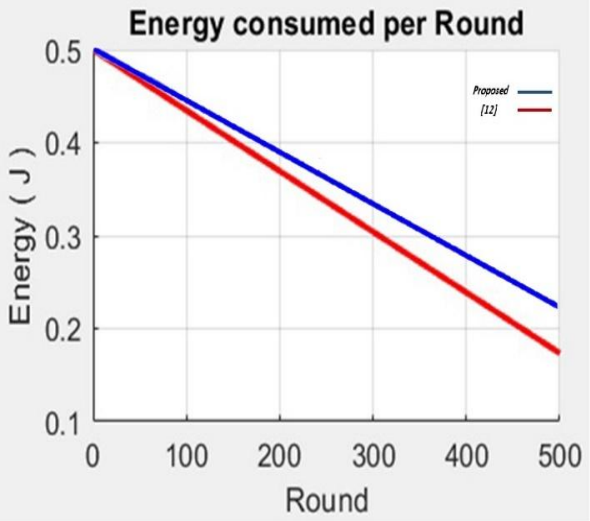

Figure (3) schema of the Energy Consumption.

Figure (4) displays the alive sensor nodes inside the network that are ready to Procedure the connection.

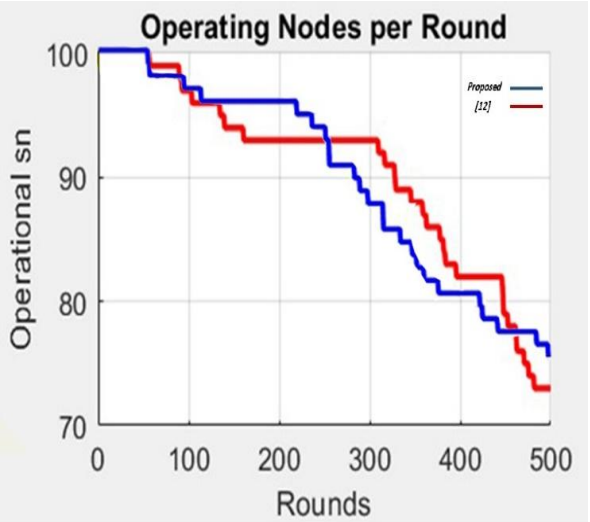

Figure (4) Displays the Alive Sensor Nodes

Figure (5) displays the dead sensor nodes that cannot take part in the communication.

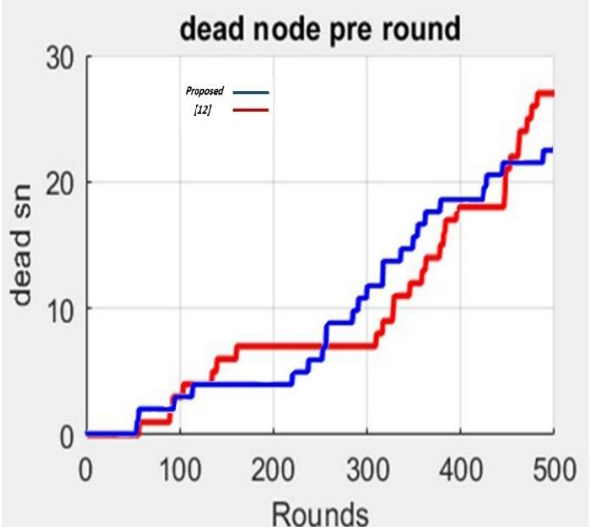

Figure (5) displays the dead sensor nodes

Figure (6) displays the time it takes to generate shared keys in comparison to the previous method, our suggested method to generate keys is light.

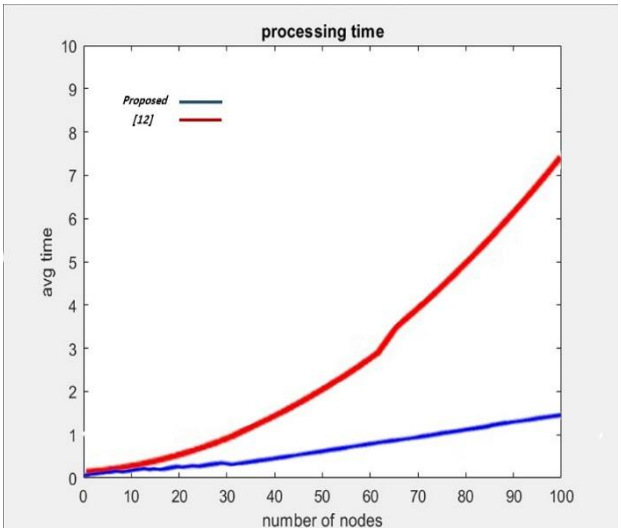

Figure (6) The Time it Takes to Generate Shared Keys

7. CONCLUSION

In this paper, we proposed secure key management to wireless sensor networks. This protocol ensures a high level of security by accomplishing (Confidentially, Authentication, Integrity) where the message is secure in each hop through (encrypted and decrypt it) from the source until it reaches the target location.

This strategy has a lot of scalability and flexibility because each sensor node has its unique key information. This method provides strong node capture resistance, and the breakthrough any the sensor node has no effect on the Remainder nodes. Resulting in a protocol that is both efficient and secure for WSN. Result utilized the sensor's resource is properly.

8. REFERENCES

[1] Al-Karaki, Jamal N., et.al. 2004, "Routing techniques in wireless sensor networks: a survey". https://homepages.dcc.ufmg.br/~loureiro/alg/092/Eduardo_RoutingTechniquesInWSNs. DOI: 1536-1284/04/$20.00 © 2004 IEEE

[2] Akyildiz, W. Su, et.al. 2002, "A survey on sensor networks," Communications Magazine, https://www.ics.uci.edu/~dsm/ics280sensor/readings/intro/akyildiz2.pdf. DOI: 0163-6804/02/$17.00 © 2002 IEEE

[3] Thiemo Voigt, Adam Dunkels, et.al. 2004, "Solar-aware clustering in Wireless Sensor Networks".http://citeseerx.ist.psu.edu/viewdoc/download. DOI:10.1.1.64.7959&rep=rep1&type=pdf

[4] K. Pavai, A. Sivagami, et.al.2009, "Study of Routing Protocols in Wireless Sensor Networks".https://ieeexplore.ieee.org/abstract/document/5376523.DOI**:** 10.1109/ACT.2009.133

[5] H.-C. Shih, J.-H. Ho, B.-Y. Liao, et.al. 2013, "Hierarchical gradient diffusion algorithm for Wireless Sensor Networks," in Recent Trends in Applied Artificial Intelligence, pp.https://link.springer.com/chapter/10.1007/978-3-642-38577-3_49.DOI: 10.1007/978-3-642-38577-3_49.

[6] Lein Harn, Sejun Song, et.al. 2019, "Hierarchical Key Management Scheme with Probabilistic Security In a

Wireless Sensor Network (WSN)" https://pdfs.semanticscholar.org/6a25/3c706e74f1dcb1a45b04a046e0ff2f5bb2bd.pdf?DOI: 10.1155/2019/3950129.

[7] Lein Harn, Sejun Song, et.al. 2017, "(Security in Wireless Sensor Networks) " https://www.researchgate.net/publication/312531334_Wireless_Sensor_Network_Security. DOI: 10.13140/RG.2.2.16684.87682.

[8] Dr. Jidong Wang, et.al, 2015, "An Efficient Key Management Scheme in HierarchicalWireless Sensor Networks" https://sci-hub.se/https://doi.org/10.1109/CCCS.2015.7374122. DOI= 10.1109/CCCS.2015.7374122.

[9] P. Raghu Vamsi, Krishna Kant, 2015," A Taxonomy of Key Management Schemes of Wireless Sensor Networks" Fifth International Conference on Advanced.https://sci-hub.se/https://doi.org/10.1109/ACCT.2015.109.DOI: 10.1109/ACCT.2015.109.

[10] Mohammed A., Ra'ad A. Muhajjar, 2018," Symmetric Key Management Scheme For Hierarchical Wireless Sensor Networks", International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.3.https://zenodo.org/record/1263077#.YgUpKN9BxPY .DOI: 10.5121/ijnsa.2018.10302. 17.

[11] Raad A. Muhajjar. 2009," SecuringWireless Hotspot Networks", Ph.D. Thesis, Jamia Millia Islamia, India.https://www.researchgate.net/publication/311858271_Securing_Wireless_Hotspot_Networks.DOI: 10.13140/RG.2.2.33302.55366

[12] Siddiq Iqbal, Prerana.S, et.al. 2019," Attack Resistant Secure Key Management in Wireless Sensor Networks", International Conference on Advances in Information Technology.https://ieeexplore.ieee.org/document/8987362. DOI: 10.1109/ICAIT47043.2019.8987362.