Key Management for Flat Wireless Sensor Network Security

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

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

ABSTRACT
Most applications use wireless sensor networksto collect data, which are considered low-cost solutions to a variety of real-world problems. Numbers of sensor nodes are deployed in a goal environment for carrying out multiple tasks. Providing confidentiality and integrity to the transmitted information through efficient key management assists. Security issues have become a critical challenge in WSNs due to the nature of the channel transport wireless and limited the resource of sensors.

In this paper, security schemes have been proposed for securing flat WSNs. The proposed scheme used a lightweight symmetric cryptographic technique that depends on a Pseudo-Random Number Generator (PRNG) to establish keys. The suggested method has a high level of security through achieving confidently in data, integrity, authentication, making efficient use of sensor resources, and providing perfect resistance to sensor node capture attacks.

Keywords
Wireless Sensor Network (WSN), flat wireless sensor networks, key management, pseudo-random number generator (PRNG), rivets cipher5(RC5)

1. INTRODUCTION
Wireless sensor networks are made up of a large number of sensors, which are tiny in size and have bounded sources after being 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 through wireless channels. The sensors send the sensed data from the surrounding area to the sink to treat it through a 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 (WSN) have received much interest for using it in a variety of applications, including military, environmental monitoring, and industrial [2].

All sensor nodes that consist it the wireless sensor networks are bounded of whence processing, connectivity, and power. As a result, one must consider this at designing a WSN. Asymmetric cryptographic algorithms are not suitable for building a safety system for a WSN due it requires a high cost [3].

Using the keys properly in the symmetric cryptosystem, we provide strong security and prevent unauthorized users from accessing the transmitted information. In this type of network, security is a challenge difficult. The cryptosystem used one secret key for encryption and decryption. [4]

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

Llanos Tobarra, Diego Cazorla, et.al In this paper, they have presented a formal approach to the security analysis of wireless sensor networks by means of a model checking tool called Avispa. The amended version of the protocol guarantees the strong freshness, authentication, message integrity, and confidentiality of the messages. this work is concerned with extending our analysis to other security protocols for wireless sensor networks such as TinySec, µTESLA, and MiniSec. [5].

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 [6].

Monika Bhalla, Nitin Pandey, et.al. This study examines security issues and vulnerabilities in wireless sensor networks and proposes the development of a new authentication protocol or technique that integrates the best characteristics of security measures.The documentprovides an overview of several wireless sensor network security techniques [7].

P. Raghu Vamsi and Krishna Kant, The authors of this research examined multiple key management techniques createdfor WSNs, as well as their taxonomy in relationtoseveral 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 [8].

3. THE PROPOSED METHOD
Building and implementing an efficient security system for a WSN is our goal, done enhancing the existing key management with a safety system that takes into account the sensors' bounded resources and conserves them 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 (BS - SN)

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

In our proposed method, the sink begins generating the shared key and authentication key, which are derived from the shared key with sensing nodes by the initial key and pseudo-random number generator(low calculate complexity) which has been tested in NIST tests.

Using the initial key, the sink encrypts the shared key and the authentication key to send both to the member nodes.

Algorithm of Pseud-Random Number Generator (PRNG)

Step1)

- Input the initial key and use java security message digest (md5) to create the hash.
- The initial key has been split into four parts p1, 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
- c1 ⟵ [bit xor (V ,F)].
- 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.

3.2 Key-Updating

The key must refresh frequently after a specific amount of time to prevent the attacker from gaining access to the current information.

So 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, and then repeats the step (3.1).

3.3 Node Addition and Deletion

When an addition new sensor node to the network. The sink will begin generating the shared key, which by the initial key and (pseudo-random number generator). As described in paragraph (3.1).

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 the task that prevents the antagonist from realizing the messages [9].

Where every sensor has, a unique (encryption/decryption) shared key as well as a unique authentication key. Furthermore, authentication and integrity have been achieved by applying a bitwise XOR to the parts that are encrypted. The key length employed in our suggested approach had 128 bits.

5. STANDARD STATISTICAL TESTS

Cryptosystems use keys that must be produced at random. Therefore, 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 [10]:

Frequency test, Serial test, Runs test, Cumulative sums test, approximate entropy test.

6. RESULT

-Figure (1) displays the random distribution of 100 nodes that are resources limited (0.5 J of Energy, thirty of range, low computational capacity) in a 100m*100m goal area, and the sink position (95, 95).

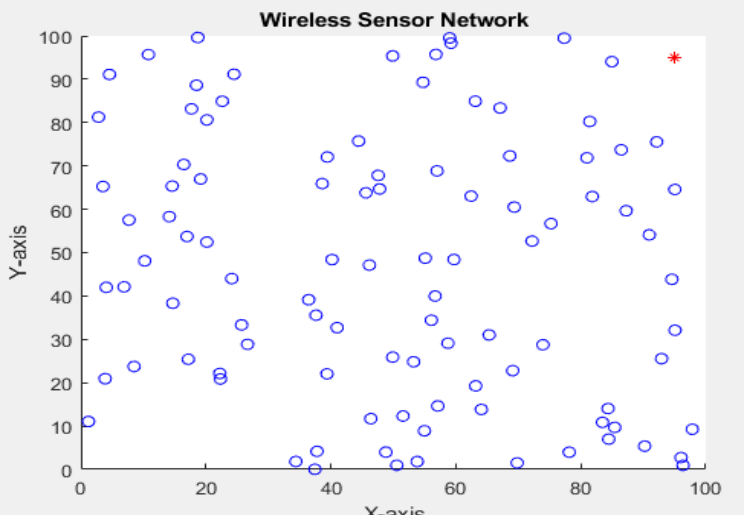

Figure (1): Random Deployment of sensor Nodes

- Figure (2) compares the energy consumed to send 15,000 packets from sensor nodes to the sink. The energy consumption in our suggested method is lower than the previous method (SPIN - part SNEP)[11-12].

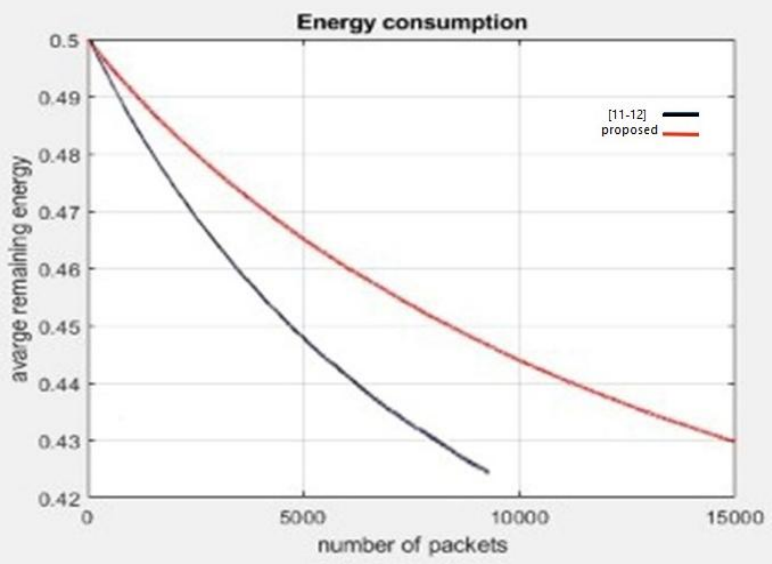

Figure (2): schema of the Energy Consumption

- Figure (3) show the time it takes for a consumer to send one packet from the source to the sink.

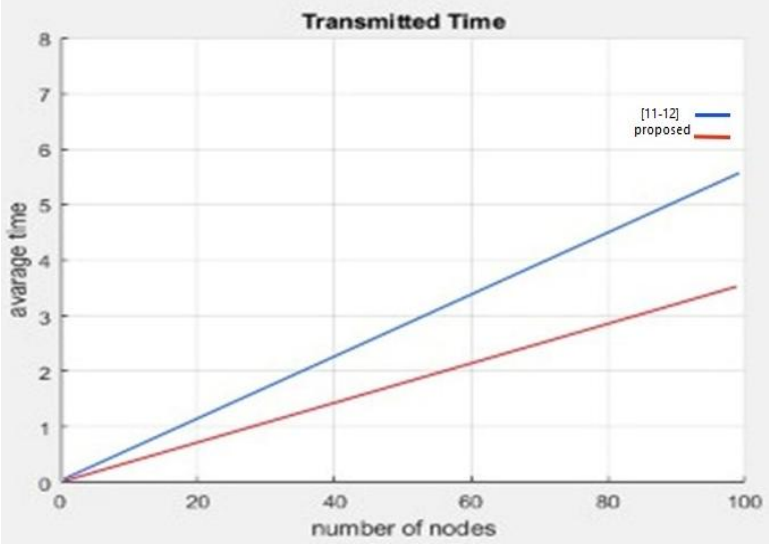

Figure (3): Average time consumers for transmitting one packet to sink.

- Figure (4) displays the time it takes to generate 100 - shared keys with a length of 128 bits. Our suggested method to generate keys is light and takes a time small than in comparison to the previous method.

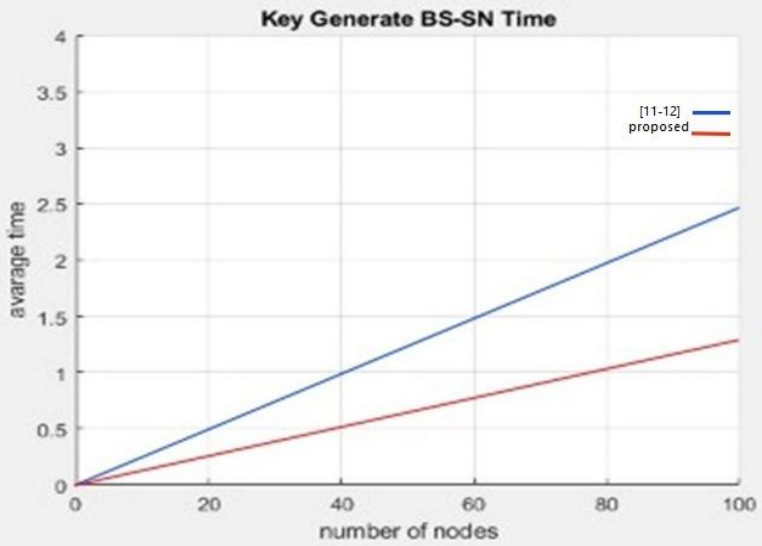

Figure (4): Time consumer for generating keys

7. CONCLUSION

In this paper, we proposed secure key management for wireless sensor networks. This protocol ensures a high level of securityby accomplishing (Confidentially, Authentication, Integrity) where the message is secure in each hop through (encrypted and decrypted) 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] I. 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] Sadaqat Ur Rehman, Muhammad Bilal, et.al.2012,"**Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSNs)**", International Journal of Computer Science,pp(96–101).https://www.scinapse.io/papers/1495968257.

[5] Llanos Tobarra, Diego Cazorla, et.al. 2007, "**Formal Analysis of Sensor Network Encryption Protocol (SNEP)**"IEEE International Conference on Mobile Adhoc and Sensor Systems.DOI:10.1109/MOBHOC.2007.4428763.

[6] Lein Harn, Sejun Song, et.al. 2017, "**SecurityinWireless Sensor Networks**" https://www.researchgate.net/publication/312531334_Wireless_Sensor_Network_Security. DOI: 10.13140/RG.2.2.16684.87682.

[7] Monika Bhalla, Nitin Pandey, et.al. 2015, "**An Efficient Key Management Scheme in Hierarchical Wireless Sensor Networks**", International Conference on Green Computing and Internet of Things.https://cibtrc.com/wp-content/uploads/2019/12/bhalla2015.pdf DOI: 10.1109/ICGCIoT.2015.7380610

[8] 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

[9] 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

[10] Raad A. Muhajjar. 2009," **Securing Wireless 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

[11] Adrian Perrig, Robert Szewczyk, et.al. 2002**," SPINS: Security Protocols for Sensor Networks"**, (part SNEP) Wireless Networks, 8, pp (521–534). https://doi.org/10.1023/A:1016598314198. DOI: 10.1023/A:1016598314198.

[12] Monika Bhalla, Nitin Pandey, et.al. 2015**," Security Protocols for Wireless Sensor Networks"**, (part SNEP) International Conference on Green Computing and Internet of Things. https://sci-hub.st/10.1109/ICGCIoT.2015.7380610. DOI: 978-1-4673-7910-6/15/$31.00.