International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 22947-22957

http://www.ripublication.com

A Novel Distributed Reprogramming Protocol In WSN

Bhanu[1]
(verma.bhanu88@gmail.com)
Dr. Mritunjay Kumar Rai[2]
(Asst. Proff.)(mritunjay.14555@lpu.co.in)
[1,2]*School of Electronics and Communication Engineering*
Lovely Professional University, Phagwara, Punjab, India (144411)

Abstract

Wireless Sensors are used to sense physical phenomenon and information is gathered and processed to obtain the relevant results. Reprogramming in Wireless Sensor Networks (WSN) is very essential. In this the new work code images are loaded to the sensor nodes. Security is the key anxiety in WSN that's why every code modernize should be genuine to avoid an aggressor from installing cruel scripts in network. In centralized approach base station is involved and if base station fails the whole process is failed. For this problem distributed reprogramming is used in which base station is not involved and several certified users can concurrently uses and reprogram the wireless sensor nodes. In this paper, a new protocol OARP (Over-Air Reprogramming Protocol) is developed and symmetric key algorithm is used. By using this protocol we improved some operations like search time of data, key-setup phase, private/public key generation phase and user signing phase.

Keywords: WSN, Security, Reprogramming, Sensor Networks, Key Generation.

Introduction

Wireless Sensor Networks (WSN) involves deploying huge quantity of small nodes which are assembly of self-structured, economical and creates network in a unstructured mode [1], [2]. Sensor nodes are great for deployment over large geographical area or in hostile environments [3]. These small price nodes could either have a permanent location or arbitrarily deployed to supervise the environment [4]. Wireless Sensor Networks (WSN) is mishmash of sensing, calculation and communication in a single tiny tool called Sensor Nodes (also known as "mote"). After sensing the environmental changes, the nodes will inform them to the other nodes over supple (flexible) network architecture [4]. The key objective of the

application is obtained by the corporation of every sensor nodes in the network. Five important features require to be considered while mounting WSN solutions: scalability, security, reliability, self-curative and robustness [5]. To calculate the physical quantity and converting it into a signal form which can readable by the observer or by any instrument, sensor nodes can be separately used. The flowing data ends at sinks (also referred as base stations). One sensor network links to another network with the help of base station (like gateway) and disseminate sensed data for further processing. Security is an enormously significant aspect when sensor network nodes are arbitrarily deployed in aggressive environment [6], [7]. Because the sensed data of sensor nodes is sensitive to various types of nasty prior to attainment base station, safety mechanisms are desired in communication part of networks to present safe data. For beneficial in-network data processing sensor networks, security is an imperative aspect. To protect such a sensed data, it becomes a complicated task. Sensor networks have the talent to function for extensive time. On occasion, it may become essential to upload new cipher picture or re-tasking offered code with dissimilar set of parameters and this process is known as reprogramming.

Cryptography

Data which is not modified and is easily understood by anyone is known as plaintext or cleat-text. The modification of plaintext so as to hide it from any attacker is known as Encryption.

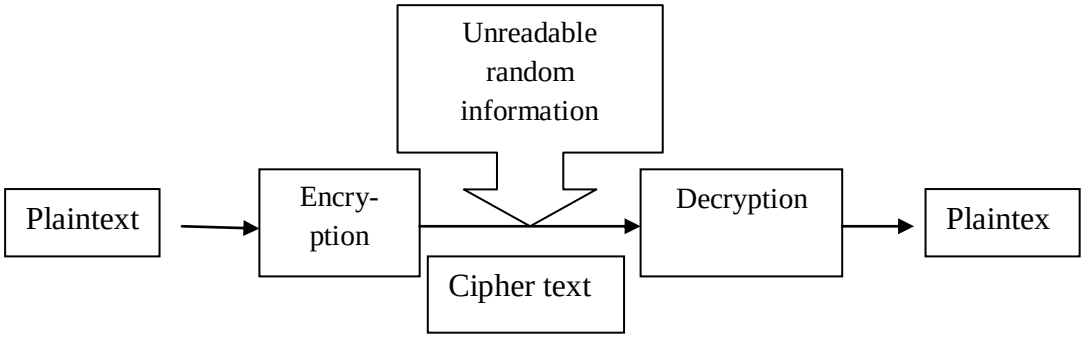


Figure 1: Cryptography Process

In encryption the plaintext is converted to cipher-text [8] and reverting the cipher-text to plain-text is known as Decryption. Let us suppose there are two parties A and B who wants to communicate with each other and they starts communication over anxious channel. They make sure that their communication residue inexplicable by anybody who may be listening. A should be definite that the information does create from B and has not been customized by anybody throughout transmission because A and B are at distant locations. The main goals that are achieved by Cryptography are:

Confidentiality: The data should not be exposed to any intentional recipients by the sensor nodes.

Data Integrity: Sometimes due to environment or nasty activities data is altered between transmissions. So in data integrity the data must not be distorted between transmissions.

Authentication: The data must be originated from the truthful source which is used in decision making device.

Types of Cryptography

Two types of cryptography techniques:

1. Symmetric Key Cryptography.
2. Asymmetric Key Cryptography.

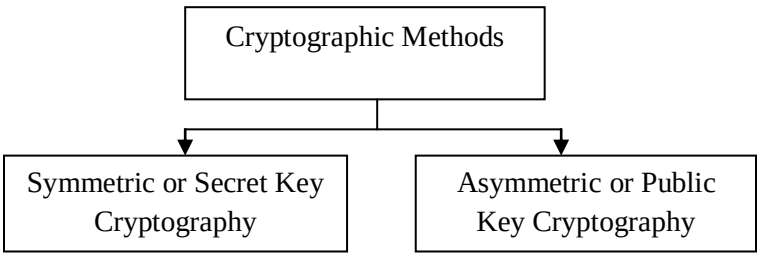


Figure 2: Cryptography Techniques

Symmetric Key (Secret Key): Suppose Alice wants to communicate with Bob. They both will use the similar key for encryption/decryption of message.

Asymmetric Key (Public Key): In this cryptography technique two keys are used: Secret Key and Public/Open Key. The secret key is reserved by recipient and the open key is publicly announced [9].

Centralized and Distributed Reprogramming

In wireless reprogramming a new code image or related instructions are loaded in sensor networks which is extremely essential process in sensor networks [10]. Protected reprogramming is most important anxiety because WSN is deployed in aggressive environment. Each code update must be authenticated so as to avoid it from unauthenticated user from installing nasty scripts in the network. All the presented protected/unprotected reprogramming protocols are related to the central approach, so it becomes essential to sustain distributed reprogramming protocols. In central approach, presence of a base station is assumed that is only base station have the right to reprogram sensor nodes. If base station or any other node loose connection with each other it becomes impossible to achieve reprogramming. Hence centralized approach is not applicable. A dispersed approach can be used for reprogramming in WSN which permits many number of certified network users to directly and

simultaneously inform cipher images on diverse nodes devoid of concerning base station [11], [12] , [13] as shown in fig. 3.

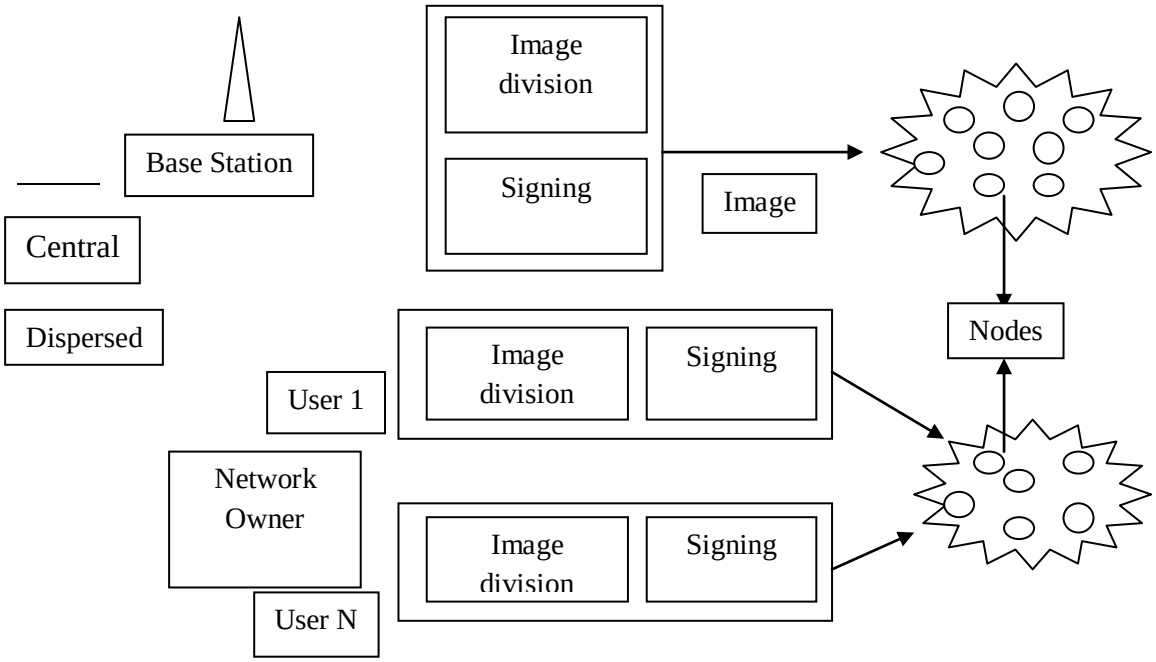


Figure 3: Outline of central and distributed reprogramming approach

Central Approach: In this approach base station is involved for transmission of data between the nodes.

Dispersed Approach: In this approach base station is not involved and many number of users can simultaneously uses code images and inform them to other nodes.

Properties of Reprogramming Protocol

- **Distributed:** The images and the codes are updated directly and simultaneously by the authorized network users and prevent unauthorized users from updating codes or images [14].
- **Freshness:** The node constantly installs new description of the program images and earlier version cannot be installed with equal or larger number of versions.
- **User Traceability:** For reprogramming, traceability is highly desirable.
- **Efficient:** Mobile sensor nodes have restricted assets (e.g. CPU processing power, bandwidth, energy). So, energy efficient and tiny storage operating cost must be given main concern to manage with resource-controlled environment of WSNs [15].

- **Scalability:** The protocol should be capable to carry large number of users and even thousands of sensor nodes in large-scale WSNs.
- **Partial reprogram ability:** To protect the sensor nodes from entirely being prohibited by network owner, unique modules on all sensor nodes cannot be over-written by anybody excluding network owner.
- **Supporting different user privileges:** To guarantee the smooth execution of WSNs, the intensity of every consumer opportunity must be restricted by network vendor. For e.g. a user is having specific identities within an exact restricted area is acceptable to reprogram the sensor nodes throughout his subscription period.

Reprogramming Protocols of Network

There are so many reprogramming protocols and three of them are given below:

a) **Deluge Protocol:** In WSN, this procedure is also known as Broadcasting/Dissemination Protocol in which huge quantity of data is transmitted from one or many source node to another nodes. This protocol is non-acknowledgement based procedure which occasionally gives information to the nodes about their surrounding states.

b) **Seluge Protocol:** It is a secure expansion to the above mentioned Distribution Protocol in wireless sensor networks. It is an open source procedure which provides safe code updating, code images. It provides security from the malicious person. It provides the authentication process i.e. when a new code is generated it provides signature to that code so as to protect from attacker. The calculation time for this procedure is more which prevents it from hacking.

c) **Distributed Protocol:** In this distributed approach no base station is involved and all the certified network users can simultaneously inform code images to the diverse nodes. Whereas in central protocol base station is involved. Sometimes the problem may occur if the base station or any other node may lose connection with each other then it becomes impossible to transmit the data. So for now a day's distributed/dispersed protocol is followed.

Brief Overview of Distributed Protocol

This distributed protocol maintains distributed reprogramming whereas all accessible protected/unprotected reprogramming protocols are related to central approach. It becomes essential to sustain distributed reprogramming in which huge amount of certified network customers can concurrently and openly renew sensor nodes without concerning base station. Three phases of this protocol are as:

System Initialization Phase: In this the network vendor defines its private and public keys [16]. The owner provides reprogramming authorities and resultant private key to authoritative user. Before deployment of the sensor nodes, only public/open parameters are encumbered on every sensor node.

User Pre-processing Phase: The reprogramming packets are created if a network customer enters WSN and has latest program cipher and then these packets are transmitted to the sensor nodes.

Sensor Node Confirmation Phase: In this, the nodes agree to the latest program code if the packet confirmation passes.

A. System Initialization Phase

1. Suppose C is a cyclical set and C_t have the equivalent prime order m. Let P be the generator of the group. Let $e=C*C$ that corresponds to C_t as a bilinear map.
2. Calculate analogous Public Key $PK_{owner}=a.P$.
3. Select two protected cryptographic Hash Functions Hf1 and Hf2 such that *Hf1: {0,1}** i.e. C and *H2: {0,1}** i.e. Z_q*.
4. Consider U_{ij} be a user identity $UID_{ij} \in \{0, 1\}*$ and public key is $PK_{ij} = Hf1(UID_{ij}\_Pr_{ij})$ and secret key $SK_{ij} = a \cdot PK_{ij}$. The network vendor transmits $\{PK_{ij}, SK_{ij}, Pr_{ij}\}$ back to U_{ij} via a protected channel [17], [18], [19], [20].

Notations

Notation Description
U_{ij}: the $_j^{th}$ network user
UID_{ij}: user U_{ij}'s identity
SK_{ij}: user U_{ij}'s private key
PK_{ij}: user U_{ij}'s public key
$SK_{owner:}$ network owner's private key
$PK_{owner:}$ network owner's public key
C: additive set
$C_{t:}$ multiplicative set
e: bilinear map C*C i.e. C_t
P: initiator of set C
m: array of set C
Hf1: hash value {0,1}* to G
Hf2: hash value {0,1}* to G_t

B. User Preprocessing Phase

The network vendor sets opportunity for the user and then finds the hash value of every packet in the page. This calculated hash value is added to the packet. The customer has to give signatures on the whole pages for confirmation/verification. The targeted node has the uniqueness set field which indicates the uniqueness of sensor nodes if the message contains the reprogramming rights which the network user requests to reprogram [21]. The code/cipher image is separated and signature is added with the code image [22]. The user U_{ij} computes the digital signatures of the message and transmits the message to the intended nodes.

C. Sensor Node Confirmation Phase

When signature message is received, each node first of all pays attention to legitimacy of programming rights and verifies that the identity of that exact node is there in the right list of user or not [23]. If available then the public parameters are verified and checks that if it is from authenticated user or not and at last verifies the data packets in code image.

Simulation and Analysis

NS2 network simulator is open source software, used for simulation and it is also a discrete event time driven simulator. NS2 uses C++ and TCL (Tool Command Language) and is widely used to simulate networking concepts. C++ is backend language and TCL is frontend language. In NS2, NAM is TCL based animatronics tool which is worn for screening network simulation traces and authentic world packet traces. It supports a variety of data inspection tools, topology outline and packet level animation. The simulation uses following parameters:

Parameter	**Value**
Type of channel	Wireless Channel
Model for Radio Propagation	Two Ray Ground
Type of Network Interface	Wireless-Phy
Type of MAC	IEEE 802.11
Type of Interface Queue	PriQueue
Type of Link Layer	LL
Antenna Model	Omni-directional Antenna
Protocol Used	OARP

The result for the average search time of the data for 2 GHz processor speed which is less than the previous 2 GHz processor speed as shown below in table 1:

Table 1:

	Previous protocol	Improved Protocol
Search Time (µs)	32.48	28.4

The execution time for 2 GHz processor for some major operations in the improved protocol as compared to previous protocol is given in table 2.

Table 2:

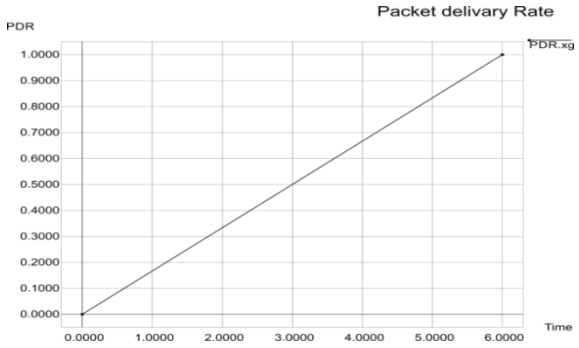
	Key Setup	Private/Public key generation of User	Signing
Time for Previous Protocol (2GHz) µs	4595.5	995.5	5211
Time for Improved Protocol (2GHz) µs	2433	801	4099

In this protocol, in addition we analyzed three more parameters which are given below:

a) Packet Delivery Ratio

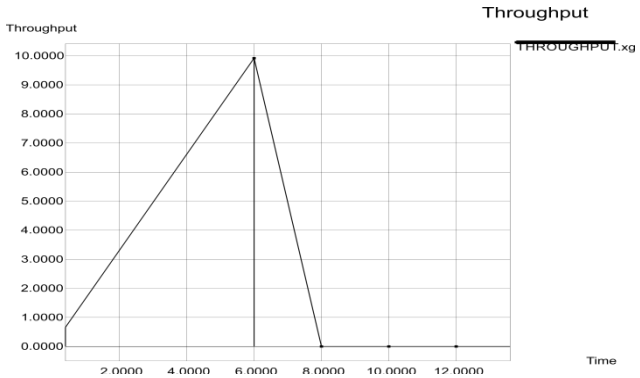
PDR means that how many data packets are successfully transmitted to the target. This will give idea about the level of delivery to destination. If the PDR is greater, the performance of the protocol is better.

PDR= Number of packets received/Number of packets transmitted



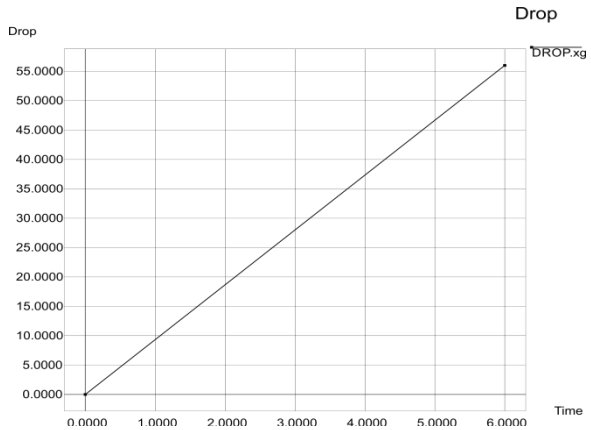
b) Throughput

When data packets are transmitted from source to destination then sometimes the packets are not transmitted due to environmental issues but successfully delivery of packets to the intended destination in presence of environmental effects is known as throughput.



c) Packet Drop

The packets are not transmitted from source to destination due to some reasons which may cause the loss of the data packet. This is known as drop of the data packet.



Conclusion

By using the above mentioned OARP protocol we improved the time for key-setup, private/public key generation of user and signing which is less than the previous protocol. In this protocol we used the processor speed of 2 GHz and compared our results with the previous 2 GHz processor speed. The improvement in Key Set-up Phase is 52.94%, in Public/Private key generation of user is 80.46% and in signing phase is 78.66%. We also calculated the average search time of data for this processor speed and the improvement is 87.43%.

Future Work

Many of secure reprogramming protocols don't support distributed operation. So this protocol has been developed which supports distributed operation.

The sensor nodes can be reprogrammed by using this protocol in a distributed manner. User can further improve the key setup, private/public key generation of user and signing according to processor speed. In some applications user would like to hide his/her reprogramming confidentiality from anybody else (as well as network vendor). So in future we can also improve the privacy in distributed reprogramming.

References

[1] S. Madria M. Tubaishat, "Sensor Networks : An Overview," *IEEE Potentials*, April/May 2003.

[2] Leonidas Guibas Feng Zhao, "Wireless Sensor Networks," *Morgan Kaufmann Publications*.

[3] W. Su, Y.Sankarasubramaniam, E. Cayirci I.F. Akyildiz, "A survey on sensor networks," *IEEE Communication Magazine*, pp. 104-112, 2002.

[4] Jamal N. Al-Karaki & Ahmed E. Kamal, "Routing Techniques in Sensor Networks: A Survey," *IEEE communications*, vol. 11, p. 628, Dec. 2004.

[5] R. C. Luo and O. CHen, "Mobile sensor node deployment and asynchronous power management for wireless sensor networks," *IEEE Trans. Ind. Electron*, vol. 59, pp. 2377-2385, May 2012.

[6] Al-Sakib Khan Pathan et.al, "Security in Wireless sensor networks: Issues and challenges," *ICACT*, pp. 1043-1048, 2006.

[7] T Newe and E Lewis M Healy, "Efficiently securing data on wireless sensor networks," *Journal of Physics: Conference Series*, vol. 76, p. 012063, 2007.

[8] Santa Mandal and Rituparna Chaki, "A Secure Encryption Logic for Communication in Wireless Sensor Networks," *International Journal on Cryptography and Information Security (IJCIS)*, vol. 2, pp. 78-82, September 2012.

[9] R. Merkle, "Protocols for Public key Cryptosystems," *Proc. IEEE Secure. Privacy*, pp. 122-134, 1980.

[10] Y. Zhu. and L. Cheng Q. Wang, "Reprogramming Wireless Sensor Networks: Challenges and Approaches," *IEEE Netw. Mag.*, vol. 20, pp. 48-55, May/June 2006.

[11] J. Chen, Y. Xiao and Y. Sun X. Cao, "Building environment control with wireless sensor and actuator networks: Centralized versus distributed," *IEEE Trans. Ind. Electron*, vol. 57, pp. 3596-3605, Nov. 2010.

[12] C. Chen, S. Chan and J. Bu D. He, "SDRP: A secure and efficient reprogramming protocol for wireless sensor networks," *IEEE Trans. Ind. Electron*, vol. 59, pp. 4155-4163, Nov. 2012.

[13] R. Han and S. Mishra J. Deng, "Secure code distribution in dynamically programmable wireless sensor networks," *Proc. ACM/IEEE IPSN*, pp. 292-300, 2006.

[14] X. Cao, P. Cheng, Y. Xiao and Y. Sun J. Chen, "Distributed collaborative control for industrial automation with wireless sensor and actuator networks," *IEEE Trans. Ind. Electron*, vol. 57, pp. 4219-4230, Dec. 2010.

[15] A. Arora, P. Sinha and H. Zhang V. Naik, "Sprinkler: A reliable and energy efficient data dissemination service for extreme scale wireless networks of embedded devices," *IEEE Trans. Mobile Comput.*, vol. 6, pp. 777-789, Jul. 2007.

[16] M. Gouda and S. S. Lam C.K. Wong, "Secure group communication using key graphs," *IEEE/ACM Transactions on Networking*, vol. 8, pp. 16-30, 2000.

[17] J. Deng, Y. S. Han, P. K. Varshney, J. Katz and A. Khalili W. Du, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Trans. Inf. Syst. Secure*, vol. 8, pp. 228-258, 2005.

[18] P. F. Oliveira and J. Barros, "Network coding protocols for secret key distribution," *Proc. Int. Symp. Information Security*, pp. 1718-1733, Nov. 2007.

[19] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Computing Surveys*, vol. 35, pp. 309-329, 2003.

[20] A. J. Menezes and S. Vanstone D. Hankerson, "Guide to Elliptic Curve Cryptography," *New York; Springer Verlag*, 2003.

[21] S. Chan, C. Chen and J. Bu D.He, "Secure and efficient dynamic program update in wireless sensor networks," *Secur. Commun. Netw.*, vol. 5, pp. 823-830, Jul. 2012.

[22] Jiangshan Yu and Qi Xie Guilin Wang, "Security Analysis of a single sign on mechanism for distributed Computer networks," *IEEE Transactions on information informatics*, vol. 9, Feb. 2013.

[23] Hui LI, Baocang WANG Xixiang LV, "Identity based key distribution for mobile Ad Hoc Networks," *Springer-Verlag Berlin Heidelberg*, 2011.