International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 8, December 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Distributed Secure Reprogramming Protocol

Vivek Soi,

SBSSTC, Ferozepur

Ramandeep

Kaur, *SBSSTC, Ferozepur*

***Abstract*—Unique from the brought together approach, a disseminated reconstructing convention comprises of three sorts of members, the system owner, approved system users, and all sensor nodes. An incorporated reinventing convention includes just two sorts of members, the base station (managed by the system owner) and all sensor nodes.**

Index Terms— Muti Direction Routing Protocol, sink, control packet, Latency, life time, PDR

I. INTRODUCTION

An incorporated reinventing convention includes just two sorts of members, the base station (managed by the system owner) and all sensor nodes. Just the base station can reinvent sensor nodes. Unique from the brought together approach, a disseminated reconstructing convention comprises of three sorts of members, the system owner, approved system users, and all sensor nodes. Here, the system owner can be disconnected. Additionally, after the users enlist to the owner, they can enter the WSN and afterward have predefined benefits to reconstruct the sensor nodes without including the owner. To give secure and appropriated reinventing, a credulous arrangement is to pre-furnish every sensor node with different public key/ reconstructing benefit combines, each of which compares to one approved client. This plan enables a system client to sign a program picture with his private key to such an extent that every sensor node can confirm whether the program picture starts from an approved client. Be that as it may, this arrangement isn't material to WSNs because of the accompanying certainties. To start with, asset imperatives on sensor nodes regularly make it unfortunate to actualize such an costly calculation. For the RSA-1024 open key cryptosystem (1024-b keys), the length of every open key is more than 1026 b. Also, for the ECC-160 [29] open key cryptosystem (160-b keys), the length of every open key is 1120 b. Accepting that the length of reinventing benefit is 32 B what's more, either RSA-1024 or ECC-160 is utilized, the length of each open key/reconstructing benefit match is more than 160 B. This implies not very numerous open key/reprogramming privilege sets can be put away in a sensor node. We consider the normally utilized MicaZ stage for instance. The 512-kB Streak memory isn't reasonable for putting away these parameters, since it is much slower and more vitality expending than ROM. On the other hand, MicaZ stage just has 128-kB ROM, while a large portion of ROM needs to be utilized for putting away program. For this situation, not very numerous users can be bolstered. Second, unmistakably the arrange owner has no capacity to predefine the reconstructing benefits of the new joining users previously the WSN organization. Once another client registers to the system owner, the owner requirements to sign another open key/reconstructing benefit combine and afterward communicates it to all sensor nodes. Clearly, this conduct isn't productive and pitifully adaptable, especially in large scale WSNs. We normally move our consideration regarding authentication based approach (CBA). Table 1.1 show the notations used in this chapter.

Notation	Descriptions
Uj	the jth network user
Sj	the jth sensor node
UIDj	the identity of user *Uj*
SKj	the private key of user *Uj*
PKj	the public key of user *Uj*
SKowner	the private key of network owner
SKj	the public key of network owner
G	a cyclic additive group
G_T	a cyclic multiplicative group
ê	a billnerar map G x G → G_T
P	generator of cyclic additive group G
q	the order of the group G
H_1	a hash function maps from {0,1} to G
H_2	a hash function maps from {0,1} to Z_q

Table 1.1 Notation used

II. System Model

Presumptions

The accompanying presumptions are considered for the proposed convention.

1. Sensors and the network user(s) (i.e., sink) are for the most part stationary after arrangement.
2. The sensor nodes are consistently circulated in the system field with arbitrary arrangement.
3. The sensors are homogeneous and have similar abilities.
4. Sensor nodes are battery fueled, consequently have constrained energy.
5. Sensor nodes can figure their leftover energy.
6. Links are symmetric, i.e., the information speed or amount is the same in both headings, arrived at the midpoint of after some time.

III. Network Model

We consider an arrangement of sensor node H_n and a sink node (network user) *Uj* with identity *UIDj* in the system. Each sensor node H_{ni} (i = 1, ..., n) has the area data (x_i , y_i).. The sink node (network user) possesses unlimited computation, memory, and battery power. The sink node (network user) also contains the id and location of each sensor node. When the sink (user) required the data from the source node, it constructs the route between them. The threshold energy is the minimum residual energy of a sensor node, beyond which; it cannot perform any additional functions except sensing and relaying the data.

IV. Security & Privacy Preservation Model

The network owner a random number s and then generate its public and private key. After that the network owner assign public key and private key for the network user. Then the network owner pre equip the public parameters into the senor node for the authentication of user before user try to update image code (reprogram) in the senor node.
The network owner assign a certificate (control packet) to the network user which gives the privilege to the user for image updation (reprogramming), has the sensor node neighbour destination table for sensing the best route between network user and sensor node, has the user identity of the network user (for user traceability) and the time stamp for freshness of the code.

4.4.1 In system initialization phase the network owner creates its public and private keys and then assigns the reprogramming privilege and the corresponding private key to the authorized user(s)

Problem 4.1: Generation of Public and Private Keys of the network owner and then assigns the reprogramming privilege and the corresponding private key to the authorized user(s).

In this phase, the network owner executes the following steps.

- Let G be a cyclic additive group generated by *P*, G_T be a cyclic multiplicative group, and G and G_T have the same primer order *q*. Let $\hat{e} : G \times G \rightarrow G_T$ be a bilinear map.
- Randomly pick a random number $s \in Z\ q$ as the master key, and compute the corresponding public key $PK_{owner} = s \cdot P$.
- Choose two secure cryptographic hash functions *H*1 and *H*2, where $H_1 : \{0, 1\}* \rightarrow G$ and $H_2 : \{0, 1\}* \rightarrow Zq$. Then, the system public parameters are $params = \{G, GT\ , \hat{e}, q, P, PK_{owner}, H_1, H_2\}$, which are loaded in each sensor node before deployment.
- Consider a user *Uj* with identity $UIDj \in \{0, 1\}$ who registers to the network owner. After verifying his registration information, the network owner first sets *Uj* 's public key as $PKj = H_1(UIDj\_Prij) \in G$ and computes the corresponding private key $SKj = s \cdot PKj$. Then, the network owner sends *{PKj, SKj, Prij}* back to *Uj* using a secure channel, such as the wired Transport.

4.4.2 In the user preprocessing, only the system public parameters from the network owner are loaded on each sensor node before deployment. In the user preprocessing phase, if a network user enters the WSN and has a new program image, he will need to construct the reprogramming packets and then send them to the sensor nodes.

Certificate-Based Approach (CBA) is used in this phase. In CBA, each user is equipped with a public-/private-key pair. Each user signs the new code image with his private key using a digital signature scheme. Also privilege given by Network owner to Network user(s) for updation of network node

Problem 4.2 : For generation of (control packet) certificate issued by network owner by using its public and private key to network user(s) by using its public and private key for reprogramming of sensor nodes of the wsn.

- To prove the user's ownership over his public key, the network owner is also equipped with a public-/private-key pair and serves as the certification authority (already assigned in algorithm 4.1).

❖ The owner issues each user, for example, Uj , a public-key certificate, which consists of the following contents:

$$Certj = \{UIDj, PKj, ExpT, SIGSK_{owner} \{h(UIDj\_PKj\_ExpT)\}\},$$

where $UIDj$ denotes user Uj 's identity, PKj indicates Uj 's public key, $ExpT$ denotes the certificate expiration time, $SKowner$ denotes the network owner's private key, and $SIGSKowner$ $\{h(UIDj\_PKj\_ExpT)\}$ is a signature over $h(UIDj\_PKj\_ExpT)$ withSK_{owner}.

❖ A broadcast message is

$$\{M, SIGSKj\{h(UIDj\_M)\}, Certj\},$$

where M denotes the updated code image andSKj denotes the private key of user Uj . For the purpose of code image authentication, each sensor node is preloaded with the owner's public key ($PKowner$) before the network deployment, and code image verification on each node contains two steps: the user certificate verification and the code image signature verification.

4.4.3 In Sensor Node Verification, upon receiving a signature message, each sensor node verifies the authentication of the user(s) and then verify the programming privilege of the network user before updating the new code image.

Problem 4.4.3 to verify the certificate of the user(s) issued by the network owner by using public params and once verification is done then update the code image.

❖ Sensor node on receives a signature message
{UIDj, Prij,m, σj},
sent by the network user(s) in algorithm (4.2)

❖ The sensor node first pays attention to the legality of the programming privilege $Prij$ and the message m.

❖ The node needs to check whether the identity of itself is included in the node identity set of $Prij$. Only if they are valid, the verification procedure goes to the next step.

❖ Given the system public parameters $\{G, G_T, \hat{}e, q, P, PK_{owner}, H_1, H_2\}$ assigned by the network owner, the sensor node performs the following verification:

$$\hat{}e(\sigma j, P) = \hat{}e\ (H2(m) \cdot H_1(UIDj\_Prij), PK_{owner})$$

❖ If the equation holds, the signature σj is valid because

$\hat{}e(\sigma j, P) = \hat{}e\ (H_2(m) \cdot SKj, P)$
here $\sigma j = H_2(m) \cdot SKj\ = \hat{}e\ (H_2(m) \cdot s \cdot PKj, P)$
here $SKj = s \cdot PKj\ = \hat{}e\ (H_2(m) \cdot PKj, s \cdot P)$
$= \hat{}e\ (H_2(m) \cdot PKj, PK_{owner})$
here $s \cdot P = , PK_{owner} = \hat{}e\ (H2(m) \cdot H_1(UIDj\_Prij), PK_{owner})$

❖ If the aforementioned verification passes, the sensor node believes that the message m and the privilege $Prij$ are from an authorized user with identity $UIDj$. Hence, the sensor node accepts the code image sent by the network user(s).

Algorithm 4.4.1 Using Elliptical Curve Cryptography Encryption and Decryption of data sent from the network user to the sensor node

create random curve and point
random curve
form = 0
a6 : 1c 5e629417 3dbdf669 b9fca0fe cd2165b0

Base point
x : c 358df1ea 9ebc2e42 2fbec069 dde73d2c
y : 9 eb318786 772fce50 72bbc1f8 22ed38bb

Creating Network User U_j (Side A) private Sk_j and Public keys PK_j

Side A secret: : c d2a3e242 4ce7401a 58e0e961 b20afcdf
Side A public key
x : 34 69023735 749bc2f7 27123ddd 13c421e8
y : 2a 82945bef 8826b76a 59602c5 1caaf73a

Creating Sensor Node H_n (Side B) private and Public keys

Side B secret: : 39 99d659e8 3428a5da 9b130925 aed734d8
Side B public key
x : 26 8856d11 8ce1eed7 2390aeae 7b3bf293
y : 1f 1f18ec52 652f16ee 9fa9b2c3 36c8422f

Creating Dummy Message data

Data to be Sent : 16 f93ff6c8 e42f891b d8aeabdf cd419f2f

Hide data on curve and send from SideA to SideB

Hidden data
x : 31 b71d6293 bb851393 2a92dbb5 fc19958c

```
y : 3d d2ff2282 87d2accb 970f677a c5c82180

Random point
x : 12 2abaa729 775cb900 bf443998 548c3e9c
y : 1e 24719fb0 5c4e03db e67be1f0 b46cac9f

Recover Transmitted Message
Received data : : 16 f93ff6c8 e42f891b d8aeabdfcd419f2f
```

V. INTRODUCTION

We lead two arrangements of trials to assess the execution of the conventions; each test was completed on the 1000m × 1000m square reenactment fields of various thickness of sensor organize and distinctive portability of sensor nodes. We executed our projects in view of the network simulator 2 (Issariyakul and Hossain 2012) (Kourdy et al. 2010). The association examples and places of nodes are haphazardly produced

VI. SIMULATION RESULTS

A proposed concept of cryptography is used to provide security preservation in wireless sensor network by hybrid encryption based cryptography to solve the privacy preservation issues. For experimentation we have used network simulator version 2 with animation for the concept of cryptography. Various parameters used for experimentation is below table 6.1:

Table 6.1: Parameters used for the experimentation

Parameters	Value
Simulator	NS2
Network Area	1200 x 1200
Simulation Time	30 sec
No of nodes	5Logical subnets
Routing Protocol	AODV (routing process)
Traffic Model	CBR
Pause Time	100 sec
Speed	11 mps
Number of sources	2
Sub-packet size	256 bytes
Transmit Power	15mW
Receiving Power	13 mW
Initial battery power	100j
MAC layer	802.11
Time Slots	Grid Distribution

The results are based on the simulation of hybrid cryptography concept in sensing field for wireless sensor network. The system test system device NS2 variant 2.33 is utilized to recreate the outcomes.

6.1.1 ENCRYPTION TIME TAKEN ANALYSIS

Experimentation has been started with cryptography in wireless sensor network communication. Figure 6.2 to Fig 6.4, showing the time taken analysis for encryption process. Comparison for the proposed work and already existing secure AODV (Bouhorma et al. 2009) & DSR scheme (Sivakumar and Ramkumar 2007) in wireless sensor network is shown in figure 6.6. The comparison shows the encryption time taken by proposed solutions is less than the already existing DSR scheme and secure AODV scheme. Normally encryption process take a lot of resources and time for their implementation but proposed scheme is showing less time so that to provide better resources management tool in wireless sensor networks.

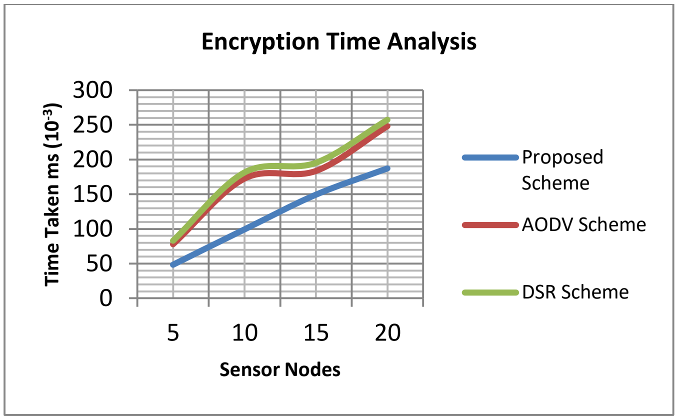

Figure 6.10: Comparison of Proposed scheme with AODV Scheme & DSR Scheme in term of Encryption Time taken

S.No	Network Density (No of Nodes)	Proposed Scheme Encryption Time Taken (mS) $x10^{-3}$	AODV Scheme Encryption Time Taken (mS) $x10^{-3}$	DSR Scheme Encryption Time Taken (mS) $x10^{-3}$
1	5	48.25	77.87	82.76
2	10	99.25	172.65	181.28
3	15	149.33	183.65	190.26
4	20	187.25	248.25	251.32

Table 6.2 Comparison table of Proposed scheme with AODV Scheme & DSR Scheme in term of Encryption Time taken

6.1.2 DECRYPTION TIME TAKEN ANALYSIS

Experimentation has been started with cryptography in wireless sensor network communication. Figure 6.11, showing the time taken analysis for decryption process. Comparison for the proposed work and already existing secure AODV (Bouhorma et al. 2009) & DSR Scheme (Sivakumar and Ramkumar 2007) in wireless sensor network The comparison shows the decryption time taken by proposed solutions is less than the already existing DSR and AODV scheme.

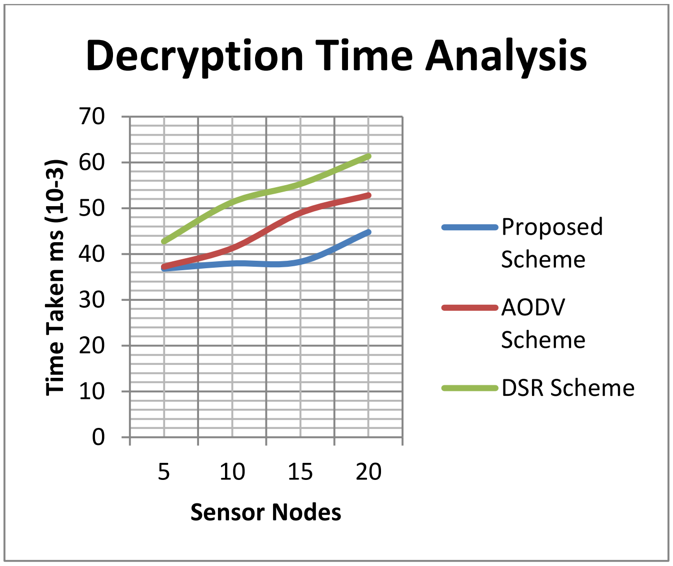

Figure 6.11: Comparison of Proposed Scheme with DSR Scheme and AODV Scheme in term of Decryption Time taken

S.No	Network Density (No of Nodes)	Proposed Scheme Decryption Time Taken (MS) $x10^{-3}$	AODV Scheme Decryption Time Taken (mS) $x10^{-3}$	DSR Scheme Dcryption Time Taken (mS) $x10^{-3}$
1	5	36.83	37.23	42.76
2	10	37.95	41.27	51.28
3	15	38.32	48.98	55.26
4	20	44.78	52.85	61.32

Table 6.3 Comparison table of Proposed scheme with AODV Scheme & DSR Scheme in term of Decryption Time taken

Normally decryption process take a lot of resources and time for their implementation but proposed scheme is showing less time so that to provide better resources management tool in wireless sensor networks.

6.1.3 KEY GENERATION TIME TAKEN ANALYSIS

Experimentation has been started with cryptography in wireless sensor network communication. Figure 6.12, showing the time taken analysis for key generation process. Comparison for the proposed work and already existing secure AODV (Bouhorma et al. 2009) & DSR Scheme (Sivakumar and Ramkumar 2007) in wireless sensor network. The comparison shows that time taken while generation of keys by proposed solutions is less than the already existing Dynamically Secured Authenticated and Aggregation scheme and secure AODV scheme.

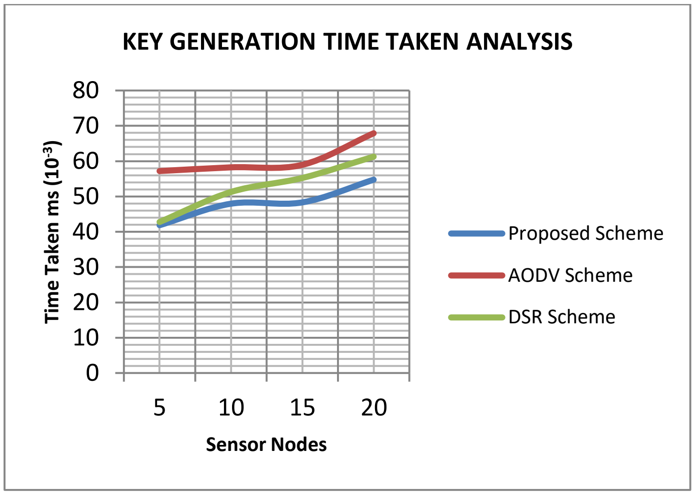

Figure 6.12: Comparison of Proposed Scheme with AODV Scheme and DSR Scheme in term of Key Generation Time taken

S.No	Network Density (No of Nodes)	Proposed Scheme Key Generation Time Taken (MS) $x10^{-3}$	AODV Scheme Key Generation Time Taken (mS) $x10^{-3}$	DSR Scheme Key Generation Time Taken (mS) $x10^{-3}$
1	5	26.83	57.23	42.76
2	10	27.95	58.27	51.28
3	15	28.32	58.98	55.26
4	20	44.78	67.85	61.32

Table 6.4 Comparison of Proposed Scheme with Dynamically Secured Authenticated &Aggregation scheme and Secure AODV Scheme in term of Key Generation Time taken

Normally generation of keys while securing process take a lot of time for their implementation but proposed scheme is showing less time so that to provide better resources management tool in wireless sensor networks.

4.7 SUMMARY

The results shown above summarized the performance of the proposed scheme for privacy preservation and secure communication in wireless sensor network DSR scheme and secure AODV scheme provide good solution for communication but proposed scheme have much better performance in saving resources, providing security and saving time for various processes in wireless sensor communication.

The energy consumption is less in case of proposed scheme processes which provided better communication in wireless sensor network as compared to the previous techniques (Sharma and Lobiyal 2015)

VII. BIBLIOGRAPHY

1. [V. C. Gungor and G. P. Hancke, “Industrial wireless sensor networks:Challenges, design principles, and technical approaches,” *IEEE Trans.Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
2. V. C. Gungor, B. Lu, and G. P. Hancke, “Opportunities and challengesof wireless sensor networks in smart grid,” *IEEE Trans. Ind. Electron.*,vol. 57, no. 10, pp. 3557–3564, Oct. 2010.
3. J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, “Distributed collaborativecontrol for industrial automation with wireless sensor and actuatornetworks,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 12, pp. 4219–4230,Dec. 2010.
4. X. Cao, J. Chen, Y. Xiao, and Y. Sun, “Building-environment control withwireless sensor and actuator networks: Centralized versus distributed,”*IEEE Trans. Ind. Electron.*, vol. 57, no. 11, pp. 3596–3605, Nov. 2010.
5. J. Carmo, P. Mendes, C. Couto, and J. Correia, “A 2.4-GHz CMOS shortrangewireless-sensor-network interface for automotive applications,”*IEEE Trans. Ind. Electron.*, vol. 57, no. 5, pp. 1764–1771, May 2010.
6. Crossbow Technology Inc., Milpitas, CA, Mote In-Network ProgrammingUser Reference, 2003.
7. J. W. Hui and D. Culler, “The dynamic behavior of a data disseminationprotocol for network programming at scale,” in *Proc. ACM SenSys*, 2004.