Security in Wireless Sensor Network

By

Vipul Kumar Dubey

12MCEI08

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

Dec 2013

Security in Wireless Sensor Network

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Computer Science and Engineering

By

Vipul Kumar Dubey

(12MCEI08)

Guided By

Prof. Sharnil Pandya

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

Dec 2013

Undertaking for Originality of the Work

I, **Vipul Kumar Dubey**, Roll. No.**12MCEI08**, give undertaking that the Major Project entitled **"Security in Wireless Sensor Network**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science and Engineering(INS)** of Nirma University, Ahmedabad, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student

Date:

Place: Endorsed by

Certificate

This is to certify that the Major Project entitled **"Security in Wireless Sensor Network"** submitted by **Vipul Kumar Dubey (12MCEI08)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science and Engineering(INS)** of Nirma University, Ahmedabad is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof. Sharnil Pandya
Guide, Assistent Professor,
Department of C.S.E.,
Institute of Technology,
Nirma University, Ahmedabad.,

Prof. Sharda Valiveti
Associate Professor, PG-Coordinator(INS),
Department of C.S.E.
Institute of Technology
Nirma University, Ahmedabad

Dr. Sanjay Garg
HOD [C.S.E. Dept.],
Institute of Technology,
Nirma University, Ahmedabad

Dr K Kotecha
Director,
Institute of Technology,
Nirma University, Ahmedabad

Abstract

Sensor Network history suggests that clustering is one of the most effective technique to increase the performance of deployed wireless sensor networks.. But along with the implementation of clustering in WSNs; it is necessary to resolve numerous challenges like secure and efficient data transmission, providing high-level security against variety of security attacks and aggregation of data. It is a challenging task to address all the challenges using a single framework or protocol. However, already few schemes like Sec-Leach, SET-IBS and SET-IBOOS have been proposed to resolve this issue but due to invention of new attacks security has always remained an unresolved issue. . In our research, after rigorous practical and theoretical analysis, we have designed an efficient timestamp-based protocol called SET-DTA to provide defence against innumerable security attacks in the clustered wireless sensor deployment environments. We have tried to address challenges like communication and computation overhead along with security to increase the performance of the deployed sensors. We have shown the feasibility of SET-DTA protocol with respect to its message size evaluation, security performance analysis, number of alive nodes, FND time, LND time and energy consumption analysis. The calculation and simulation results are also provided to carry-out the detailed analysis and discussion of the proposed scheme. .

Acknowledgements

My deepest thanks to **Prof. Sharnil Pandya** , Assistent Professor, PG-Coordinator(INS), Department of Computer Science and Engineering, Institute of Technology, Nirma University, for giving me an opportunity and guidance throughout the project. It was only due to her valuable opinion, cheerful enthusiasm and ever friendly nature that I was able to do part of my research work in a respectable manner.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr. Ketan Kotecha**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.

I would also thank my Institution, all my faculty members in Department of Computer Science.

I would like to thank my colleagues for being with me and help me.

Vipul Kumar Dubey

12MCEI08

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

In general wireless sensor network is the network of low-cost, low-power, and multi-functional wireless sensing devices. These devices are deployed in geographical field and collected information about sound ,temperature and other environmental conditions and send it to the destination.

The importance of WSN is increasing exponentially and WSN have been regarded as basic infrastructures for future universal communications due to a variety of nascent potential applications monitoring plants and environment, the health status of humans, animals,control and instrumentation of industrial machines along with detection of chemical and biological threats and leaks etc.

There are two ways for communication in wireless sensor network centralized and decentralized. In centralized communication techniques base station plays key role and all the communication takes place through base station, base station works as a mediator in these communications. In decentralized communication , sensor nodes are communicate with each other by cluster head (cluster head presents in each sub-networks called clusters). Cluster head receives the message from it's cluster and send it to the base station. Non-clustered techniques are more viable for sensor nodes for

communication in this technique sensor nodes can communicate with their surrounding nodes directly(authentication by base station compulsory before communication)

1.2 Motivation

In a cluster-based WSN (CWSN), it is a better approach to keep a powerful base station which can compute or store large amount of data if required. The reason behind this approach is sensor nodes present in the respective clusters are equipped with limited energy and memory requirements and once they are deployed these nodes also need to process data of their neighbouring nodes as well. Researchers have been widely studying CWSNs in the last decade in the literature, however, the implementation of the cluster-based architecture in the real world is rather complicated [31].

After rigorous analysis of previously proposed protocols like LEACH, Sec-LEACH [20], RLEACH [21], GS-LEACH [22], SET-IBOOS [31], SET-IBS [31], we have reached to the conclusion that all these schemes can easily address routing issues present in the WSNs but they have limited scope to provide security against high-level security attacks is still an opportunity to carry-out a detailed research and implement a cost-effective efficient solution. From these results, we have also found that most of the security attacks can be protected or avoided by time-stamp based authentication schemes [1].

In this paper, we have also addressed an issue of orphan node problem by using asymmetric key mechanism rather than symmetric key mechanism for CWSNs. Mainly security of CWSNs can be divided into three categories: [i] base station security [ii] cluster-based security [iii] sensor node security. To address all these security issues, we have divided the proposed security protocol SET-DTA into two processes: a) authentication process b) session establishment process.

1.3 Project Defination

In our project we are designing a time-stamp based protocol named 'SET-DTA'..This protocol provides security for the transmission in decentralized wireless sensor networks.Our proposed protocol has divided into two stages: Authentication and session establishment. In the duration of authentication phase, communication initiating by the sender by sending it's own identity and other encrypted details (encrypted by sender's private key) to the receiver. Receiver node can verify the details about sender with the base station anytime during the initiated communication link and can also verify sender node's signature and timestamps difference ().In second phase, for establishing a session between sender and receiver , a unique session number and a unique session key will be generated.

. The initiation or entry of other sensor nodes during the current session is protected by this protocol ,the protocol also protect the deployed wireless sensor network from diverse security attacks in term of lifetime.

The primary objective of the proposed protocol SET-DTA is to assure a secure and efficient data transmission between clusters, sensor nodes present in the respective cluster and a base station(s). Though there has been so many researches done in the area of security still until today to provide strong protection against newly evolved security attacks is a vital issue. In this paper, to the certain extent, we aim to solve the problem of security by implementing timestamp based protocol and new version of El-gamal digital signature scheme using random numbers.

Chapter 2

Literature Survey

2.1 Wireless Network Arrangements

A wireless sensor network has a fixed base station and a large number of wireless sensor nodes which has similar capability and functionality[23] and we our assumption that BS is always reliable and trusted authority. In a wireless sensor network surrounding nodes could be compromised by variety of security attacks, these attacks affect the data transmission between sensor nodes and a base station. In non-clustered scenario base station is responsible for data aggregation and storage and any sensor node can communicate with surrounding sensor nodes only via the medium of base station. But in clustered scenario sensor nodes are divided into clusters and communication takes place via cluster-head(CH) of an individual cluster via the medium of a base station(s)[1-4]. In all discussed cases it is advisable to switch the sensor nodes into inactive or sleep mode when it is not a part of active communication for saving energy.

2.2 Protocol preambles

In WSN the protocols related to data transmission always leave vulnerability to a number of security attacks[6-7].Noticeable attacks like cloning , node capture to sensor nodes could result in serious damage to the network and may cause of the huge

packet loss. If an attacker has compromised or pretended an original node , it can provoke such high level attacks and results in disrupting the network .Apart from this an attacker could intend to inject malicious packets in the deployed WSN and can leak the confidential data outside the network. To provide security against all these attacks we has designed an efficient time-stamp based protocol named SET-DAT ,it is robust against insider and outsider both type of attacks .The proposed scheme mitigate the attacking risks and increase worry of an attacker to identify and compromise important nodes present in WSN. The most of the transmission protocol does not provide emphatic security against newly evolved security attacks, but in our proposed protocol we aim to overcome this problem by using the timestamp and digital signature based crypto-system that guarantees assurance and strong defence against variety of security attacks by also considering energy aware information exchange in WSNs

Chapter 3

Literature Survey And Implementation Methodology

3.1 SET-DTA Scheme for CWSNs

In this section, we introduce the new version of IBS scheme by using new version of El-gamal digital signature authentication scheme for the random numbers. Here, we have modified the conventional IBS scheme and used asymmetric encryption scheme to mitigate the problem of orphan node in CWSNs. In order to reduce the communication and computational overhead during the digital signature signing and verification process, we have introduced novel timestamp based solution. The digital signature scheme which has been used in the implementation of this protocol uses the public key cryptography for encryption and signature verification. For each user there is a secret key x and corresponding public keys are α, β, p *where*[20] :

$$\beta = \alpha^x mod p.(i)$$

Here, α, β *and* p *are publics keys which are kept public and* x *will be kept secret.*

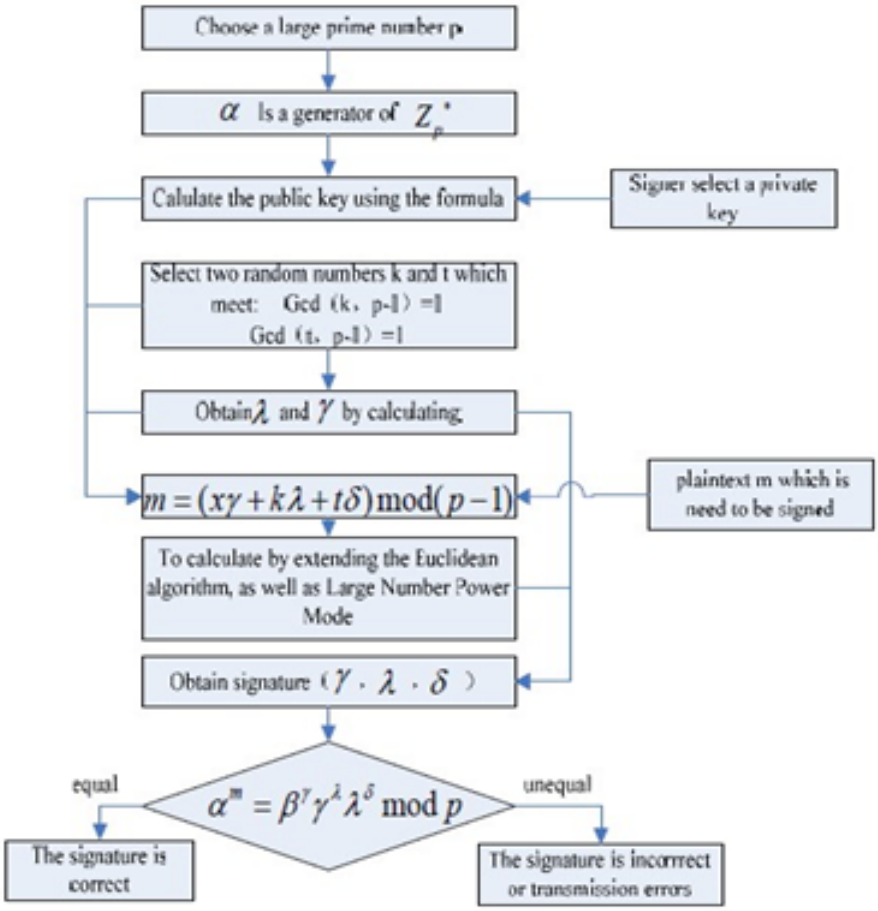


Figure 3.1: : Digital Signature Generation using El-Gamal [44]

3.2 Implementation Tool

3.2.1 TOSSIM: A Simulator for TinyOS Networks[44]

TOSSIM is a discrete event simulator for TinyOS sensor networks.Instead of compiling a TinyOS application for a mote,we can compile it into the TOSSIM framework,which runs on a PC.TOSSIM's primary goal is to provide a high delity simulation of TinyOS applications.For this reason , it focuses on simulating TinyOS and it's execution ,

rather than simulating real world.

3.3 Implementation methods

3.3.1 PROPOSED SET-DAT SCHEME FOR WSNs

The proposed protocol scheme has been divided into two processes: (i) Authentication process (ii) Session establishment process. However, the functioning of the proposed protocol SET-DTA has been divided into four steps:

- **Initial Setup**: The BS (as a trust authority) acts as a master key generator(msk) and public parameters , and p for the private key generator (PKG), these keys will be distributed to all sensor nodes.
- **Key Management**: A sensor node generates a private key DIDA with its own identity using msk.
- **Signature signing**: Given a message Msg, sending time-stamp ts, current time-stamp tc generates a signature SIG.
- **Signature Verification**: Generated signature will be verified in two modes: (i) valid and (ii) invalid.

If signature is valid, than communication can moves to the further stage session establishment and outputs accepted otherwise process will be terminated. The detailed description of the proposed scheme is given in the following section.

3.3.2 Proposed Protocols Functioning Procedure

The proposed SET-DTA scheme has following procedural steps:

System Initial Setup Procedure : The step by step description of the proposed SET-DTA scheme is as follows:

- First of all, BS registers all the valid sensor nodes and also generates private key for all the register nodes,
- In addition, Base Station also registers all the verified users and created their private keys.
- When a sensor node A registers with the base station, it keeps the record of sensor nodes by storing the identity of sensor node with the sending time-stamp Ts.
- To provide the additional security against various attacks the BS sends registration information encrypted with the hash function H like (H (SIDA), Ts)
- After receiving the broadcasted information from the Base Station, all the sensor nodes present in the network will reply by sending their acknowledgements respectively. In addition, if a sensor node will not receive any information, it wont send any ACK to the Base Station. To the all silent nodes, the base station immediately resends the message again. In this proposed scheme it is assumed that the Base Station will never store generated secret keys of sensor nodes and users.

Authentication Process After successful registration of a sensor node, authentication process will be performed by the receiving nodes. In this scheme, authentication is very important process as it provides strong defence against various security attacks. After completion of the successful authentication procedure, both sending and receiving sensor nodes will generate their session key. The generation of the session key procedure is described in the remainder part of this protocol. The steps of the initiated authentication process is given below and also shown in Figure 1.

- **Step 1**. As shown in Figure 1, the sensor node A sends a communication request to Sensor node B. To initiate secure communication, we have encrypted

the communication message with the private key of the sending sensor node as shown in equation (i). We have also included sending timestamp TS in the encrypted message.

Step 1 ((Identity SIDA, Sign S, Message M), Secret key DIDA) .. (i)

- **Step 2** After receiving communication request, receiving node B will verify the identity of the sending sensor node A. a. After the verification, before sensor node B sends the reply message, it will calculate the time-difference (ΔT) *between* Tc $(Current\ timestamp)$ *and* Ts $(Sending\ time - stamp)$.
  $We\ have\ set\ a\ threshold\ on\ the\ time - difference\ if\ it\ is\ less\ than$ 10 $milli -$ *seconds then sensor node B will send its identity along with its timestamp and signature else go to the Step* 1 *again.*

step 2 Check the Sensor node A is register with BS Signature Verify (Identity SIDA, Sending timestamp Ts sign S, message M, secret key SIDA)?.. .. ..(ii)

Step 2a Calculate (Tc-Ts) and check (Tc-Ts)> maximum time difference (ΔT)?.....(iii)

- **Step 3** After the authentication process, sensor node B will reply by sending reply message which includes identity SIDB, signature S and message M encrypted with the secret key DIDB.

Step 3 ((Identity SIDB, Sign S, Message M), Secret key DIDB) .. (iv)

- **Step 4** Now, sensor node A will perform the same steps as Step2 and verify the registration of sensor node A and again calculate the time-difference (ΔT)
  between Tc $(Current\ timestamp\ and\ Ts$ $(Sending\ time - stamp)$
  as explained in following equations.

Step 4a: Check the Sensor node B is register with the Base Station,

Signature Verify

((SIDB,TS),DIDB,S P)... .. (v)

Step 4a: Calculate (Tc-Ts) and check (Tc-Ts)> time difference (ΔT)?.....(*vi*)

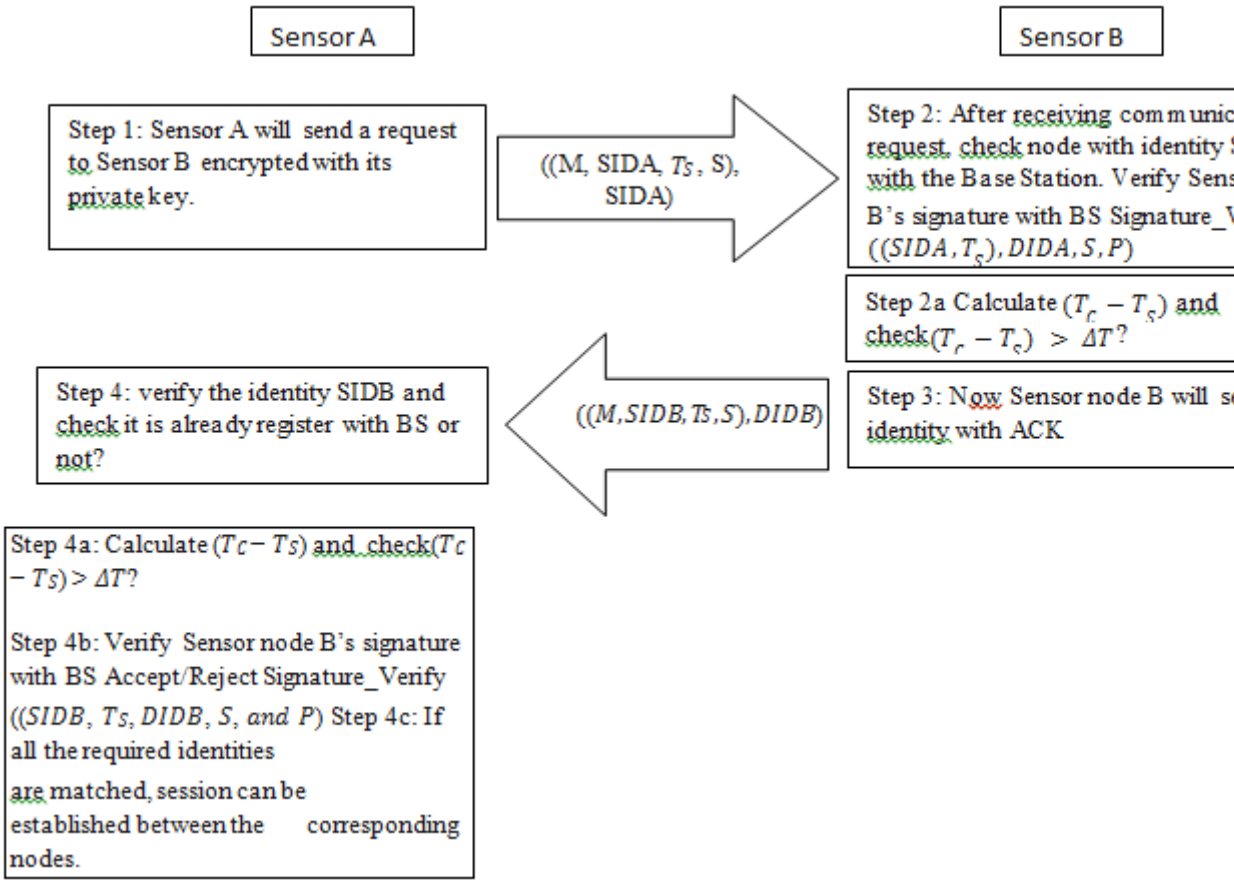


Figure 3.2: Authentication Process

The proposed scheme have used certain terminologies. The meaning of these terminologies is given in the following table:

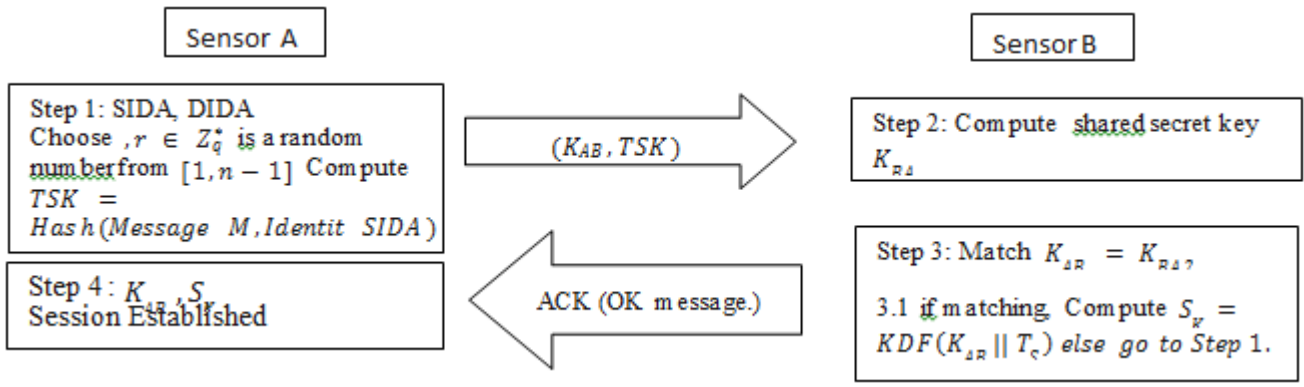


Figure 3.3: Session Establishment Process

3.3.3 Session Key Establishment Process

To increase the level of security, we have established unique session key management scheme for each session as shown in Figure 2. The process of the session key establishment is given below.

Step 1. This process will be initiated by selecting a random number r Zq and compute the Temporary Session key TSK encrypted with the hash function.

Step 1. Choose r Zq compute TSK=Hash(message M, identity SIDA).....(vii)

Step 2. After receiving session establishment request, sensor node B will generate a shared secret key KBA and compare it with KAB to check it is matching or not.

Step 2: KBA shared secret key generation.....(viii)

Step 3. If it is matching, sensor node B will compute the session establishment key SK = KDF (KAB || TS) using the key generation function KDF which is based on RSA algorithm. here, KDF can be defined by [9] RSA key GENERAtion function.

Step 3: Match KAB = KBA 3.1: if both KAB=KBA is matching, compute SK = KDF(KAB || Ts).....(ix)

Step 4. Now, we can use the established session key to secure a session between sensor node A and B. It will also provide additional security to manage concurrency so third party sensor node or intruder cannot enter the session and perform attacks

like node capture, cloning etc.

Step 4: Utilization of the session key generated in the previous step and concurrency management...(x)

MSKBS	Master Secret Key For Base Station
SIDA	Identity of sensor node for node A
DIDA	Secret key for sensor node A
PKBS	Public Key For Base Station
UIDA	Identity of user A
UPKA	Private Key of user A
M	Communication message
BS	Base station
Hash	hash function
||	Concatenation
K	Security parameter
S	Signature of the user
Ts	Sending time-stamp
Tc	Current time-stamp
UPKA	Private Key of user A
KAB	Common shared secret between node A and B on node A
TSK	Temporary key
T	Maximum time-difference
SK	Session key
KDF	Key derivation function
WSNs	Wireless Sensor Networks
J	Jouls
Kbps	Kilo bytes per second
dB	Decibels
mV	milli volts

Table I: Description of different terminologies used in this proposed SET-DTA protocol

Chapter 4

Experimental Analysis and Results

4.1 Security Analysis

To evaluate the security of the proposed protocol SET-DTA, we have analyzed various range of security attacks and the scenarios when a malicious node exists in the network and try to intercept the communication between the sensor nodes. In the remainder part, we have described how this proposed protocol can provide strong defence against various adversaries and attacks.

4.1.1 Node Compromosing attacks

Such attacks and attackers are considered as the most threaten adversaries. Such attackers can access the secret information stored in the compromised nodes, e.g., private or public keys, session keys, node identities etc. [6 and 25].

4.1.2 Passive Attacks

Attacks like eaves dropping, traffic congestion can be initiated during anytime of the wireless network deployment. Such passive attackers can also monitor the network and can prepare themselves for carrying-out future attacks [2-3].

4.1.3 Active Attacks/Real-time Attacks

Active attackers have greater ability than passive adversaries, which can tamper with the active wireless channels. Therefore, the attackers can forge, reply and modify messages [1]. Nowadays in WSNs, attackers have started implementing numerous active attacks like bogus and replayed routing attacks, node-capture attack, cloning attack etc. [21-29 and 40].

4.2 Protocol Characteristics and Features

In this section we have done the quantitative analysis of the message size (transmitted packet) used in the conducted experiments. Transmitted packet p consist of following parameters shown in Table 2 and TinyOs parameters as shown in Table 3. We have carried-out all the experiments in two ways: Mica2 Sensor Kit and Sensor Simulators: Tossim and Castallia [39X]. The total size of the message ranges from 4045 bytes. The quantitative calculation of the message size is shown below.

Total Size of the message $=|SIDAp| + |Ti| + |R| + |V|$ ranges from 40-45 bytes. . (xiii)

4.3 Experimental Result

For all the experiments we have used mica2 and mica2dot motes. For better performance analysis, we have also done various experiments on Tossim Simulators and tested from 50 to 1000 deployed sensor nodes as shown in the following figure. For energy analysis, we have used Castallia simulator as Tossim simulator does not support energy model [40]. The metrics we have used to test our experimentation results are Energy consumption, FND (first node dies) time, LND (Last node dies) time and number of alive nodes as shown below:

Sr. No.	Parameters	Description	Size(bytes
1	SIDAp, p is transmitted packet	Node identity of the transmitted packet p	2 bytes
2	Ts	Sending time-stamp	2 bytes
3	Tc	Current time-stamp	2 bytes
4	R	Message Size	10-15 byte
5	Key size	ECC over prime field(Fp)	160-bit
6	V	Variable	Approx. bytes

Table I: Message Size Evaluation

Sr. No.	Parameters	Size
1	Max. Message Size	40-45 bytes(as per equation (xxii))
2	Radio data rate	19.2 kbps
3	Power Out	0 dB/mV
4	Duty Cycle	100 percent

Table II: TinyOs Parameters [39]

4.3.1 Message Size Comparison

Message size for the transmission is very important parameter as it determines the computation workload and efficiency of the protocol. We can see the detailed comparison in Figure 3.

4.3.2 FND Time

FND means time when the first node in WSN dies. It is important as this simulation time suggests the initiated deterioration of the deployed wireless sensor networks as

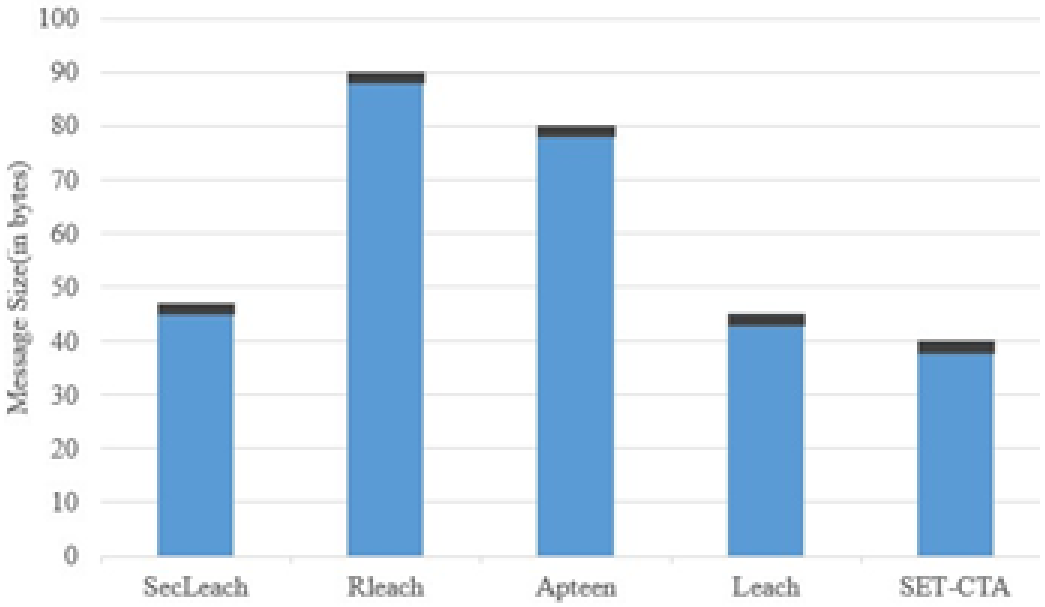


Figure 4.1: Comparison of Message Size in different security schemes.

shown in Figure 4.

4.3.3 LND Time

LND means time when the whole network will become inactive or say when all the sensor nodes will become inactive. Here we have evaluated the proposed protocol with other standard energy efficient protocols [21-25] as shown in the following Figure 5.

4.3.4 Number of Alive Nodes

The ability of sensing and collecting information in a WSN depends on the set of alive nodes [1]. Here we have done rigorous theoretical and practical analysis and identified number of alive nodes of SET-CTA protocol and also compared it with other methodologies as mentioned below in Figure 6:

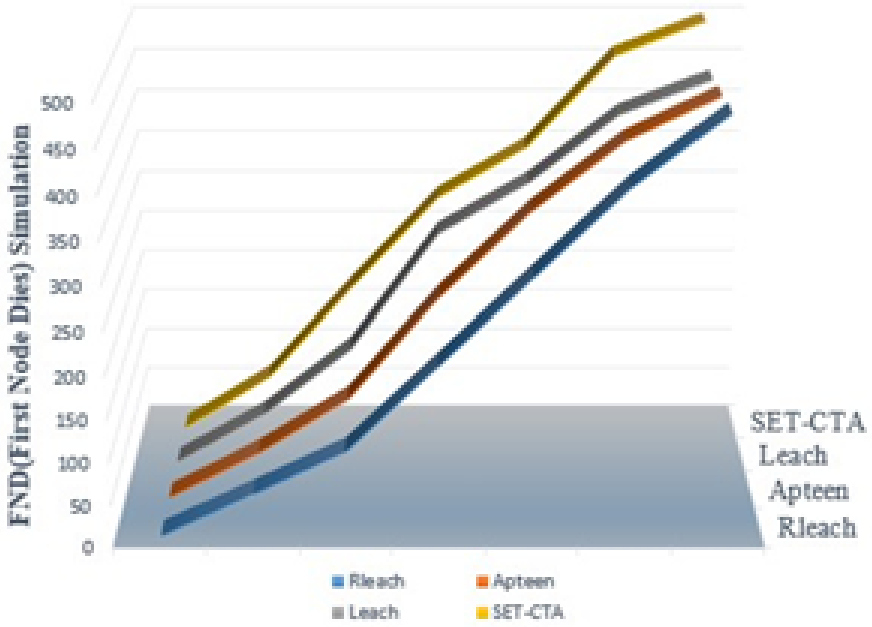


Figure 4.2: Comparison of FND Time in different security schemes.

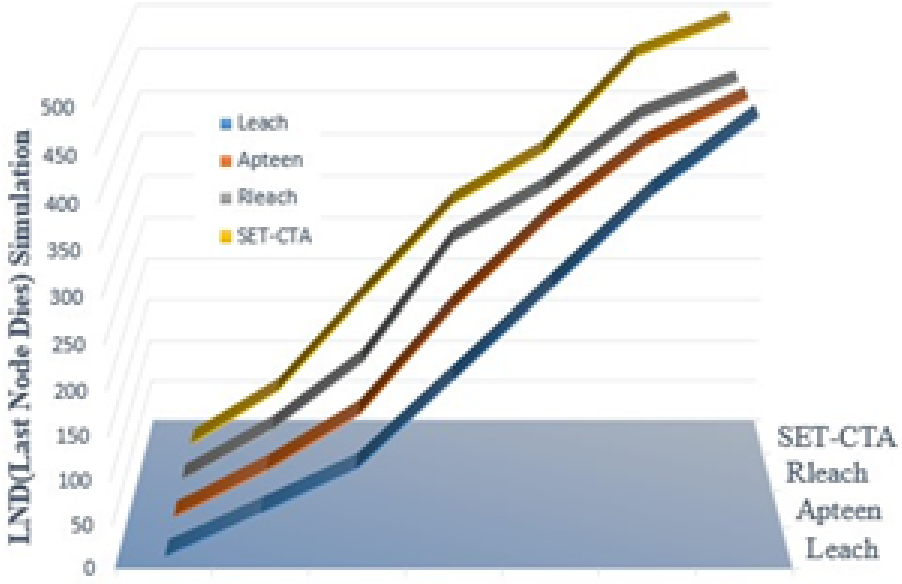


Figure 4.3: Comparison of LND Time in different security schemes.

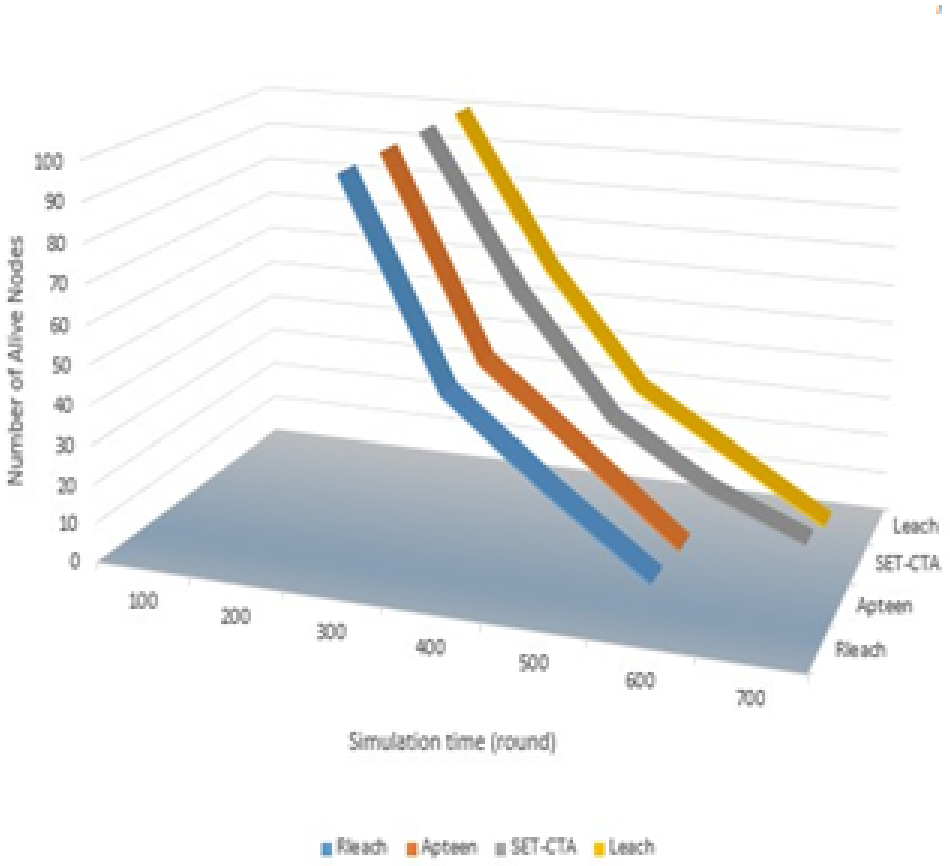


Figure 4.4: Comparison of Alive Nodes in different security schemes.

4.3.5 Energy Consumption Analysis

As we all know, along with providing good security it is important to minimize the energy consumption workload. SO here we have done detailed analysis and compared various methodologies as shown below in Figure 7 :

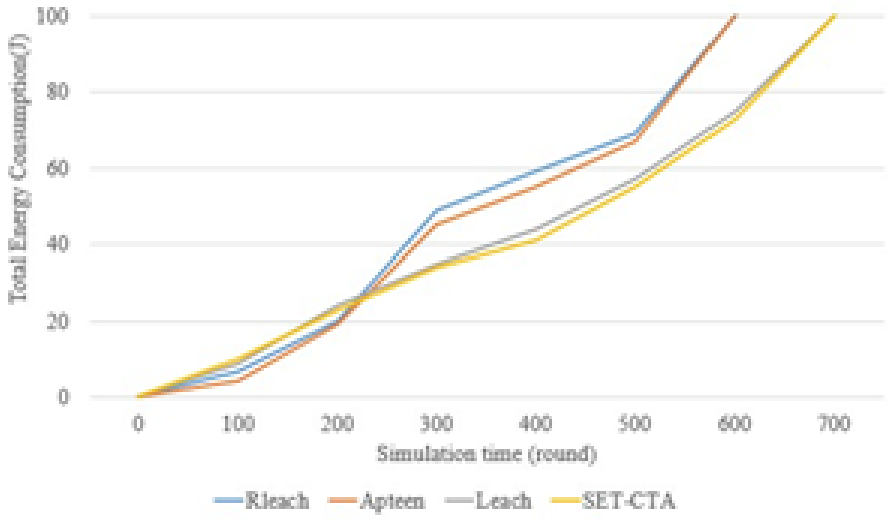
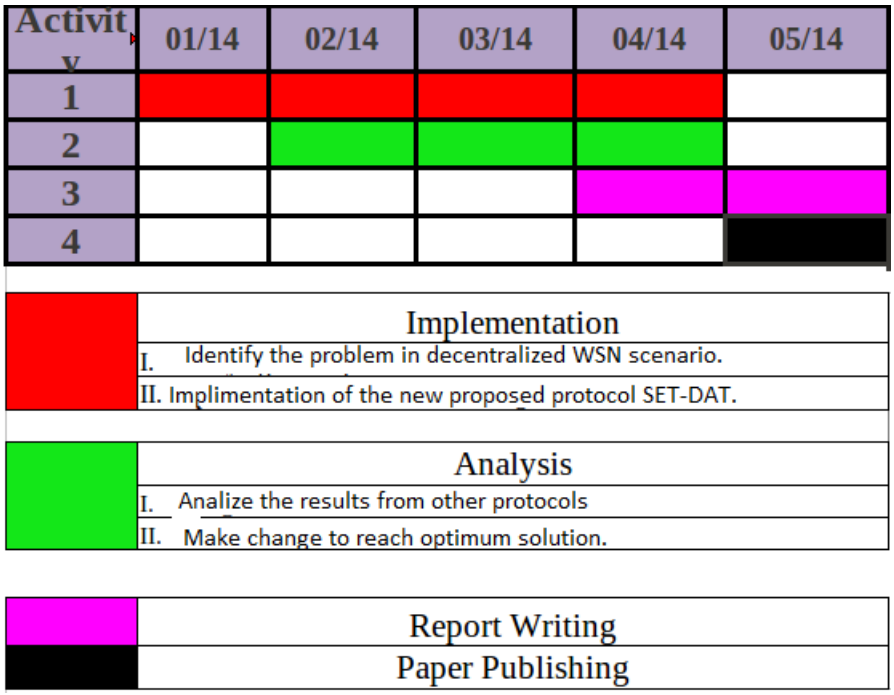


Figure 4.5: Energy Consumption Analysis.

Chapter 5

Time Line for Project Completion



Chapter 6

Conclusion and Future Work

6.1 Conclusion

We have followed various security challenges, security strike and dissected different Leachlike approachs in concentrated remote sensor situations. We then proposed incorporated timestamp based security convention called "SET-DTA", examined its aspects, different uninvolved, dynamic and hub bargaining ambushes. In the assessment area, we have assessed the proposed "SET-DTA" convention against various security assaults, security philosophies [43], correspondence and processing overhead. We have additionally given answers for give solid protection against extensive variety of security assaults by utilizing elliptic bend crypto-framework over prime field FP, concurrency administration plan, timestamp based verification plan and session key foundation plan. Finally however not slightest, we have contrasted the proposed convention and the most recent examination philosophies as far as transmitted parcel size, FND time, LND time, number of alive hubs and vitality utilization utilizing different realtime Mica2 sensor pack and test system results; inevitably we have demonstrated that this plan fulfills elevated amount security prerequisites required in militaries or government associations and it is additionally effective regarding correspondence and calculation workloads. In future, we are wanting to propose the comparative sort of

answers for the decentralized remote sensor situations.

6.2 Future Work

In future, we are planning to propose the similar kind of solutions for the decentralized wireless sensor environments.In decentralized communication also we will consider the communication and computation overhead along with analysis of several security attacks and provide wide range of security by using elliptic curve crypto-system in prime-field.For secure communication in decentralized scheme we will provide concurrency management scheme, timestamp based authentication scheme and session key establishment scheme.

Bibliography

[1] L. Huang, J. Li, M. Guizani, Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks, IEEE Trans. Parallel and Distri. Syst., 2012.

[2] Modares, Hero; Salleh, Rosli; Moravejosharieh, Amirhossein;, "Overview of Security Issues in Wireless Sensor Networks," Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on , vol., no., pp.308-311, 20-22 Sept. 2011.

[3] Xiaowang Guo; Jianyong Zhu; , "Research on security issues in Wireless Sensor Networks," Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on , vol.2, no., pp.636639, 12-14 Aug. 2011

[4] HongShan Qu; Wen Liu; , "A robust key predistribution scheme for wireless sensor networks,"Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.634-637, 27-29 May 2011

[5] Wang Hai-Chun; Huang Tao; , "Design of Security Gateway Based on Chaotic Encryption," Internet Technology and Applications (iTAP), 2011 International Conference on , vol., no., pp.1-4, 16-18 Aug. 2011.

[6] Burgner, D.E.; Wahsheh, L.A.; , "Security of Wireless Sensor Networks," Information Technology: New Generations (ITNG), 2011 Eighth International Conference on , vol., no., pp.315-320, 11-13 April 2011.

[7] Vithya, G.; Vinayagasundaram, B.; , "Actuation sensor with adaptive routing and QOS aware checkpoint arrangement on Wireless Multimedia Sensor Network," Recent Trends in Information Technology (ICRTIT), 2011 International Conference on , vol., no., pp.444-449, 3-5 June 2011

[8] Akerberg, J.; Gidlund, M.; Bjorkman, M.; , "Future research challenges in wireless sensor and actuator networks targeting industrial automation," Industrial Informatics (INDIN), 2011 9th IEEE International Conference on , vol., no., pp.410-415, 26-29 July 2011.

[9] Sahana, A.; Misra, I.S.; , "Implementation of RSA security protocol for sensor network security: Design and network lifetime analysis," Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on , vol., no., pp.15, Feb. 28 2011-March 3 2011.

[10] Junqi Duan; Yajuan Qin; Sidong Zhang; Tao Zheng; Hongke Zhang; , "Issues of Trust Management for Mobile Wireless Sensor Networks," Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on , vol., no., pp.1-4, 23-25 Sept. 2011.

[11] Sheela, D.; Priyadarshini; Mahadevan, G.; , "Efficient approach to detect clone attacks in Wireless sensor etworks," Electronics Computer Technology (ICECT), 2011 3rd International Conference on , vol.5, no., pp.194-198, 8-10 April 2011

[12] Ullah, F.; Ahmad, M.; Habib, M.; Muhammad, J.; , "Analysis of security protocols for Wireless Sensor Networks," Computer Research and Development (ICCRD), 2011 3rd International Conference on , vol.2, no., pp.383-387, 11-13 March 2011

[13] Iram, R.; Sheikh, M.I.; Jabbar, S.; Minhas, A.A.; , "Computational intelligence based optimization in wireless sensor network," Information and Communication

Technologies (ICICT), 2011 International Conference on , vol., no., pp.16, 2324 July 2011.

[14] Ning, H.; Liu, H.; Mao, J.; Zhang, Y.; , "Scalable and distributed key array authentication protocol in radio frequency identification-based sensor systems," Communications, IET , vol.5, no.12, pp.1755-1768, August 2011.

[15] Yang, Piyi; Cao, Zhenfu; Dong, Xiaolei; Zia, Tanveer A.; , "An Efficient Privacy Preserving Data Aggregation Scheme with Constant Communication Overheads for Wireless Sensor Networks," Communications Letters, IEEE , vol.15, no.11, pp.1205-1207, November 2011

[16] Fan Wu; Hao-Ting Pai; Xinxin Zhu; Pei-Yun Hsueh; Ya-Han Hu; , "Dynamic access control for secure group communication in wireless sensor networks," Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2011 8th International Conference on , vol., no., pp.288-291, 17-19 May 2011.

[17] Bechkit, W.; , "New key management schemes for resource constrained wireless sensor networks," World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a , vol., no., pp.1-3, 2024 June 2011

[18] Benzaid, C.; Saiah, A.; Badache, N.; , "Secure pairwise broadcast time synchronization in wireless sensor networks," Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on , vol., no., pp.1-6, 27-29 June 2011 .

[19] Ortolani, S.; Conti, M.; Crispo, B.; Di Pietro, R.; , "Events privacy in WSNs: A new model and its application," World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a , vol., no., pp.1-9, 20-24 June 2011.

[20] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, An analytical model for information retrieval in wireless sensor networks using enhanced APTEEN protocol, IEEE Trans. Parallel Distrib. Syst., vol. 13, 2002.

[21] S. Yi, J. Heo, Y. Cho et al., PEACH: Powere cient and adaptive clustering hierarchy protocol for WSNs, Comput. Commun. vol. 30, no. 14-15, 2007.

[22] L. B. Oliveira, A. Ferreira, M. A. Vilaca et al., SecLEACH-On the security of clustered sensor networks, Signal Process. vol. 87, 2007.

[23] P. Banerjee, D. Jacobson, and S. Lahiri, Security and performance analysis of a secure clustering protocol for sensor networks, in Proc. IEEE NCA, 2007.

[24] K. Zhang, C. Wang, and C. Wang, A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management, in Proc. WiCOM, 2008

[25] D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing, in Lect. Notes. Comput. Sc. - CRYPTO, 2001.

[26] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, in Lect. Notes. Comput. Sc. - CRYPTO, 1985

[27] S. Xu, Y. Mu, and W. Susilo, Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security, in Lect. Notes. Comput. Sc. - Inf. Secur. Privacy, 2006.

[28] C.-K. Chu, J. K. Liu, J. Zhou et al., Practical IDbased encryption for wireless sensor network, in Proc. ACM ASIACCS, 2010.

[29] Y. Lee and S. Lee, A new efficient key management protocol for wireless sensor and actor networks," Arxiv preprint arXiv:0912.0580, 2009.

[30] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, Group-based key management for mobile sensor networks," in Proc. IEEE Sarnoff Symp., pp. 1-5, 2010.

[31] A. Willig, "Wireless sensor networks: concept, challenges and approaches", Elektrotechnik Informationstechnik, 2006.

[32] C. Cordeiro, D. Agrawal," AD HOC SENSOR NETWORKS: Theory and Applications", book Published by World Scientific, 2006.

[33] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, Wireless Sensor Network Security: A Survey, Security in Distributed, Grid and Pervasive Computing 17:367-388, 2007. [2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam.

[34] Jianmin Zhang , Wenqi Yu and Xiande Liu ,CRTBA: Chinese Remainder Theorem-Based Broadcast authentication in Wireless Sensor Networks,2009.

[35] Mark Hempstead, Michael J. Lyons, David Brooks, and Gu-Yeon Wei, Sur-vey of Hardware Systems for Wireless Sensor Networks,Journal of Low Power Electronics Vol.4, 110, 2008.

[36] Elaine Shi and Adrian Perrig, Designing Secure Sensor Networks, IEEE Wireless Communications, December 2004.

[37] Mohsen Sharifi, Saeed Sedighian Kashi and Saeed Pourroostaei Arda-kani,LAP: A Lightweight Authentication Protocol for Smart Dust Wireless Sensor Networks,2008.

[38] G. Anastasi, M. Conti*, A. Falchi, E. Gregori*, A. Passarella, Performance Measurements of Mote Sensor Networks, CNR-IIT Institute, Italy, 2005

[39] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks, vol. 1, no. 2-3, 2003.

[40] S. Even, O. Goldreich, and S. Micali, On- Line/Off-Line Digital Signatures, in Lect. Notes. Comput. Sc. - CRYPTO, 1990.

[41] K. Wandra, S. Pandya, Survey on security in wireless sensor networks, International Journal of scientific engineering research, vol 3, issue 12, December 2012.

[42] D. Liu and P. Ning, Multilevel mTESLA: Broadcast authentication for distributed sensor networks, ACM Trans. Embed. Comput. Syst., vol. 3, no. 4, pp. 800836, 2004.

[43] Prabu, M. and Shanmugalakshmi, R.; A Comparative and Overview Analysis of Elliptic Curve Cryptography over Finite Fields, ICIMT, IEEE conference on information and multimedia technology, pp. 495-499, 2009.

[44] http://docs.tinyos.net/index.php/TOSSIM, Description: a webpage introduced TOSSIM.