Centralized Timestamp based Approach for Wireless Sensor Networks

K. H. Wandra, Ph.D
Principal, Department of Computer Science and Engineering, C. U Shah College of Engineering, Wadhwan, Gujarat, India

Sharnil Pandya
Research Scholar, School of Engineering, R K University,
Rajkot, India
and
Department of Computer Science and Engineering, Nirma University Sarkhej-Gandhinagar Highway, Gujarat, India

ABSTRACT

Sensor Network has gained the reputation of becoming the most promising technology of 21st century due to its low cost and ability to traverse longer distances in unattended hostile environments. However, security has still remained a burning and an unresolved issue for both centralized and decentralized wireless sensor networks. Using rigorous theoretical and practical analysis, we have traced numerous security challenges, security attacks and have designed an efficient timestamp-based protocol called "SET-CTA" to provide defense against variety of security attacks in non-clustered wireless sensor deployment environments. Previously proposed TESLA and μ-TESLA [40] schemes were limited in scope; those schemes were only able to provide protection against basic security attacks like non-repudiation. But SETCTA scheme gives a flexibility to provide protection against numerous security attacks like (e.g. eavesdropping, node capture, man in the middle attack, con-currency attacks, trust attacks and many more [40]) by considering various timestamp based parameters like current-timestamp, sending time-stamp, timestamp-difference(Δt) etc. To the best of my knowledge, this is the only end-to-end timestamp based scheme that can provide secure and efficient transmission in centralized wireless sensor environments and can also assure protection against different range of security attacks.

General Terms

Security, Authentication

Keywords

Centralized, Current-timestamp, Sending-timestamp, secure and efficient data transmission protocol, FND (First Node Dies) time, LND (Last Node Dies) time, Elliptic Curve Cryptography.

1. INTRODUCTION

In general, wireless sensor networks are networks of distributed autonomous, inexpensive and disposable (reusable or rechargeable) devices that can sense, monitor or process numerous data such as sound, temperature and motion [1]. Such individual nodes are spatially distributed to sense and monitor the physical changes of the surrounding environment and they are also capable to communicate in wireless sensor networks in two ways: centralized and decentralized. Centralized means such data processing and transfer can be carried out through or via the medium of a base station in WSNs. Whereas, in the case of decentralized environments, Sensor nodes are spatially distributed in different clusters and can only communicate with other sensor nodes with the help of Cluster Head (CHs) present in each of the clusters. After receiving messages from neighboring sensor nodes, cluster head of that cluster can finally send the received messages to a base station. However, in nonclustered scenarios, it is feasible for sensor nodes to communicate with other surrounding nodes directly but only after permission or required authentication done by a base station(s). Generally in such non-clustered scenarios, trust is a major issue [10]; so to initiate trustworthy communication between the neighboring sensor nodes it is important to do the pre-registration and authentication of all the sensor nodes present in the network.

1.1 Background and Motivations

To deal with different type of wireless environments, it is mandatory to provide high-level security to these kinds of networks with an efficient security framework or a proactive protocol. So after the rigorous theoretical and practical analysis of innumerable security challenges, attacks and detailed literature survey, we have been able to introduce an efficient timestamp-based protocol called 'SET-CTA' to provide secure and efficient transmission in centralized wireless sensor environments. As we all know, different security applications have diverse security requirements so it is a challenging or almost invincible task to satisfy all the security requirements using a single authentication protocol. So we did a detailed survey and found that most of the security attacks can be protected or delayed by time-stamp based authentication schemes [19]. The problem with the previously developed time-stamp based schemes was their inability to provide security against vast range of security attacks even though their computational requirements were less. So we have designed a novel protocol called "SET-CTA" to provide high-level protection for the confidential security applications used in militaries or government organizations. Detailed literature depicts that numerous protocols have been proposed such as APTEEN [20], PEACH [21], Sec-Leach [22] which use similar concepts of LEACH protocol [1]. In this research paper, we have represented such methodologies as Leach-like methodologies. Most of Leach-like methodologies make use of the symmetric key management schemes for security but it cannot provide defense against security attacks like cloning, selective forwarding, node-capture, trust [40 and 10]. In this research paper we have used acronym "high-level security attacks" for the above mentioned security attacks. To increase the level of protection, digital signature can be used as very effective security mechanism in critical applications like military services or government agencies.

In the recent years, the concept of digital signature has been developed as a good authentication practice in WSNs for security. Carman [25] has first tried to combine the features of IBS and key predistribution schemes into WSNs and some other research methodologies have also been evolved in recent years, e.g., [4], [5], [34], [30] and [36]. But all these schemes were unable to provide security against wide range of security attacks. SETCTA scheme has been proposed in order to increase the protection against high-level security attacks by also considering communication and computational overhead. A general method for constructing online/offline signature schemes was introduced by the researcher Even et al. [41] before few years. The proposed scheme can be very effective for the key management [30] and security using ID based authentication [28]. Specifically, the given scheme can be executed on a sensor node or at the BS prior to communication and also during communication [1]. Some IBS schemes are designed for WSNs afterwards, such as [28] and [29].

In this proposed scheme, we have divided this protocol into two stages: authentication and session establishment. During the phase of authentication, sender sensor node will initiate the communication with the receiver sensor node by sending its own identity and other details encrypted with its private key. Moreover, receiver sensor node can always verify the details of the sender node with the base station anytime during the initiated communication link. Not only this, receiver sensor node can also verify sender sensor node's signature and the timestamp difference (Δt). In the second phase, a unique session number will be generated and unique session key will be generated to establish a session between sender and a receiver node. This protocol will protect other sensor nodes to initiate or enter into the current session and protect the deployed wireless sensor network from variety of security attacks in terms of network lifetime.

The remainder of this paper is organized as follows. Section 2 describes the wireless network arrangements, security preambles and vulnerabilities. Section 3 introduces the SETCTA scheme. Section 4 present the details of the proposed SET-CTA features and characteristics. Section 5 analyzes and evaluates the proposed SET-CTA protocol. The last section concludes the proposed work.

2. NETWORK PROTOCOL ARRANGEMENTS AND PREAMBLES

2.1 Wireless Network Arrangements

Here, we have considered a wireless sensor network which consists variety of wireless sensor motes and a base station(s). Before we go further we assume that the BS is always reliable and a trusted authority. Moreover, all the surrounding sensor nodes may be compromised by variety of security attacks and such high-level security attacks also affect the data transmission between sensor nodes and a base station. In case of Nonclustered environments, here, base station is the central entity and it is responsible for data aggregation and storage. In this environment, sensor nodes can communicate with the surrounding sensor nodes via the medium of a base station(s). Whereas, in the case of CWSNs, sensor nodes are divided into homogenous clusters and communication can be done via cluster-head (CH) of an individual cluster via the medium of a base station(s) [4]. In all these cases, thus, it is advisable to switch the sensor nodes into sleep or inactive mode when it is not sending or receiving any data for saving energy. In this paper, the proposed SET-CTA are designed for non-clustered wireless environments.

2.2 Protocol Preambles and Security Vulnerabilities

As per the latest research work analysis [1-43], it is analyzed that the protocols used in WSNs are vulnerable to a variety of security attacks like cloning, node capture etc. Such attacks may result in serious damage to the network and may lead to huge packet loss. If an attacker (malicious sensor node) manages to compromise or pretend to be an original sensor node, it can provoke such high-level attacks and results in disrupting the network. In addition, an attacker may intend to inject malicious packets in the deployed WSN and can transmit confidential information outside the network. To provide defense against all these attacks we have designed an efficient time-stamp based protocol called "SET-CTA", which is robust against insider as well as outsider attacks than other type of protocols in WSNs [41]. The characteristics of the proposed scheme mitigate the attacking risks and increase the headache of an attacker to identify and compromise important nodes present in WSNs.

The primary objective of the proposed protocol SET-CTA is to guarantee a secure and efficient data transmission between neighboring sensor nodes and a base station(s). Meanwhile, most of existing secure transmission protocols for WSNs in the literature [5-10], are not capable to provide strong protection against newly evolved security attacks. In this paper, we aim to solve this problem by using the timestamp and digital signature based crypto-system that guarantees assurance and strong defense against variety of security attacks by also considering energy aware information exchange in WSNs.

3. IBS SCHEME AND SET-CTA FOR WSNs

In this section, we introduce the digital signature scheme and SET-CTA scheme used in the paper. It is important to note that the conventional schemes are specifically designed to satisfy security requirements or energy requirements. But by concentrating on one of the above requirements conventional protocols have failed to comply required protection in WSNs, e.g. leach-like methodologies [20-25]. To satisfy both security and energy requirements for WSNs, we adapt the conventional IBS scheme and have also developed a protocol that require less energy requirements and can switch the sensor nodes in sleep state when it does not transmit any data in the network. In order to further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional digital signature scheme for WSNs [1 and 28] based on elliptive curve cryptography for prime field Fp, where p is a prime number. The equation of the elliptic curve over prime field Fp is defined as [41]: y^2 (mod p)=(X^3+aX+b) mod p, Where: ($4a^3+27b^2$)mod p $\neq 0$ and x,y,a,b ∈ [0 ,p-1]. The points on elliptic curve E are denoted as: E (Fp)={ (x,y):x,y ∈ Fp Satisfy $y^2= x^3+ax+b$ } ∪ {0}.

3.1 Point Addition for Elliptic Curve over fp:

$$x_R = \left(\lambda^2 - x_P - x_Q \right) mod\, p,$$

$$y_R = (\lambda(x_P - x_R) - y_P) \, mod\, p,$$

$$Where, \lambda = \frac{y_Q - y_P}{x_Q - x_P} \, mod\, p$$

Point Doubling for Elliptic Curve over fp:

$$x_R = (\lambda^2 - 2x_P) \, mod \, p,$$

$$y_R = (\lambda(x_P - x_R) - y_P) \, mod \, p,$$

$$Where, \lambda = \frac{3x_p^2 + a}{2y_p} \, mod \, p$$

4. PROPOSED SET_CTA SCHEME FOR WSNs

An IBS scheme implemented for WSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing of the data transmitting nodes, and verification of the data receiving nodes [1]. In this proposed protocol has used signature based algorithm which consist of four different processes such as initial system setup, key management, signature generation and signature verification.

4.1 Proposed Protocol Operation

SET-CTA protocol operates in number of stages during communication. Each stage consists of an authentication phase and a session establishment phase. We assume that, all the sensor nodes have knowledge of the starting and ending timestamp of each stage, because of the time synchronization.

4.1.1 System Initial Setup Procedure

The step by step description of the proposed SET-CTA scheme is as follows:

a. First of all, BS registers all the valid sensor nodes and also generates private key for all the register nodes,

b. In addition, Base Station also registers all the verified users and created their private keys.

c. 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.

d. To provide the additional security against various attacks the BS sends registration information encrypted with the hash function H like (H (SIDA),

T_S).

e. 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 won't 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.

4.1.2 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 defense 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 Fig.1.

Step1: 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. We have also included sending timestamp T_S in the encrypted message.

Step2: 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 T_c (Current timestamp) and T_s (Sending time stamp). We have set a threshold on the time difference, if it is less than 10 milli-seconds than sensor node B will send its identity along with its timestamp and signature else go to the Step 1 again.

Step3: 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.

Step4: 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 T_c (Current timestamp) and T_s (Sending time stamp).

The proposed scheme have used certain terminologies. The meanings of these terminologies are given in the following table 1.

Table 1. Description of different terminologies used in this proposed SET-CTA protocol

Symbol	Interpretation
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
T_S	Sending time-stamp
T_C	Current time-stamp
KAB	Common shared secret between node A and B on node A
TSK	Temporary key
ΔT	Maximum time-difference
S_K	Session key
KDF	Key derivation function

WSNs	Wireless Sensor Networks
J	Joules
Kbps	Kilo bytes per second
dB	Decibels
mV	milli volts

4.1.3 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.

Step 1. This process will be initiated by selecting a random number $r \in Z_{q^*}$ and compute the Temporary Session key TSK encrypted with the hash function.

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 3. If it is matching, sensor node B will compute the session establishment key $SK = KDF\ (KAB \parallel TS)$ using the key generation function KDF which is based on RSA algorithm.

Here, KDF can be defined by [9]:

```
RSA_key_Generation_Function {

Select two large primes p and q such that $p \neq q$

$\eta \leftarrow p * q$
$\Phi(\eta) = (p - 1)\ (q - 1)$

Select e such that $1 < e <$ (η) and e is coprime to $\Phi(\eta)$

$d \leftarrow e - 1 mod\ \Phi(\eta)$    // d is inverse of e modulo   Φ(η)

$Public\ key \leftarrow (e, n)$    // To be announced publicly

$Private\ key \leftarrow d$      // To be kept secret    Return Public_key and Private_key.

 }
```

Step 3: Match $K_{AB} =$? If both $K_{AB} = K_{BA}$ is matching, compute SK.

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.

5. IBS SCHEME AND SET-CTA FOR WSNs

This section describes SET-CTA protocol characteristics and features, security analysis and various sensor-kit simulation results.

5.1 Protocol Characteristics and Features

In this section, we summarize the characteristics of the proposed SET-CTA protocol. Figure 1 and 2 shows the general procedure and steps of the proposed SET-CTA protocol. We have done rigorous practical and theoretical analysis of the proposed protocol to evaluate its performance. All the analyzed characteristics are as follows.

5.1.1 Authentication Procedure

Secure authentication procedure based on current and sending timestamp has been followed to achieve strong authentication against high-level security attacks. [31-39].

5.1.2 Communication Overhead

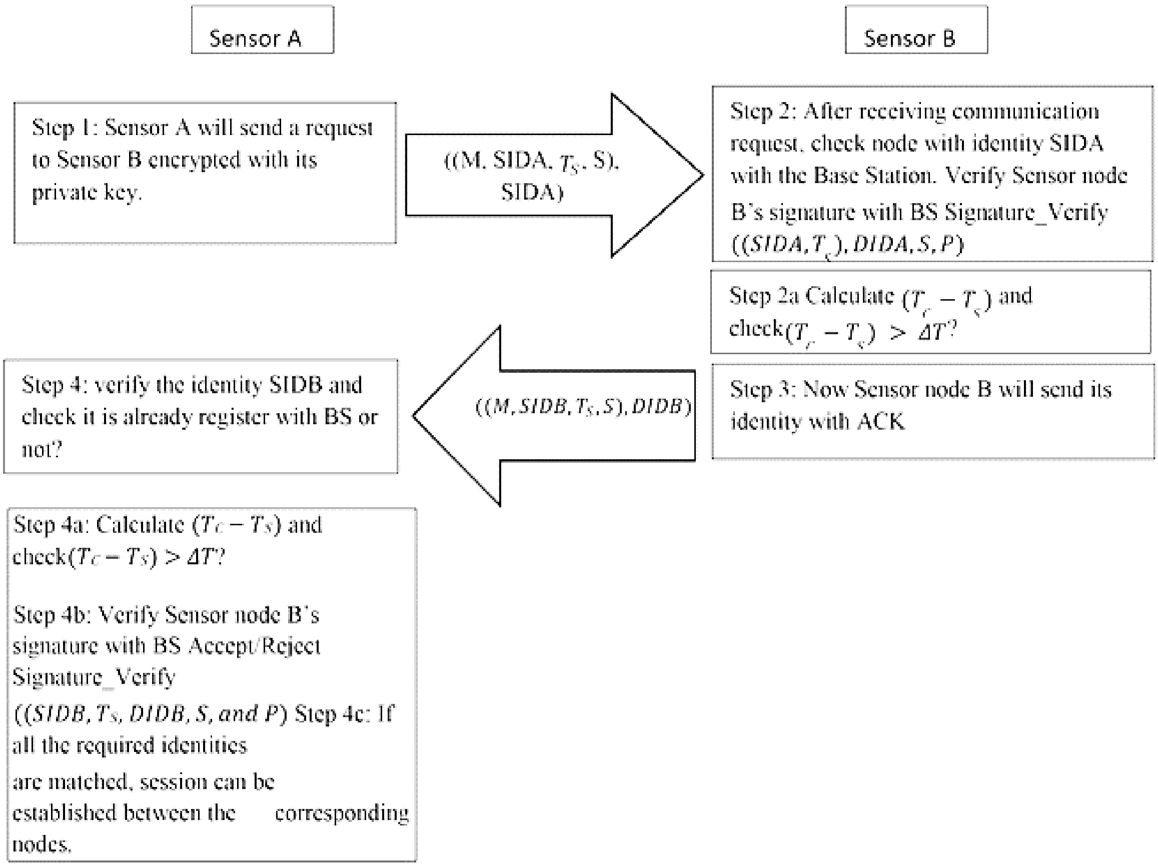
This protocol assures less communication overhead as all the required mechanisms like digital signatures, public and private keys are stored on the base station(s).

5.1.3 Computation Overhead

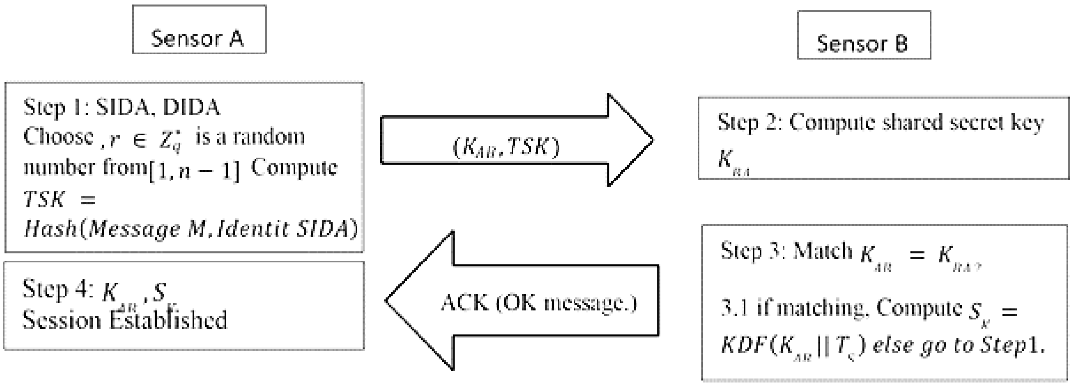
We have designed this protocol in such a way that it assures secure and efficient transmission between the sensor nodes and a base station(s).

5.1.4 Protection against Security attacks

This proposed scheme very much focused on providing a strong defense against high-level security attacks like node capture attack, cloning attack etc. [1-9]. Macintosh, use the font named Times. Right margins should be justified, not ragged.


Sensor A
Sensor B
Step 1: Sensor A will send a request to Sensor B encrypted with its private key.
((M, SIDA, T_S, S), SIDA)
Step 2: After receiving communication request, check node with identity SIDA with the Base Station. Verify Sensor node B's signature with BS Signature_Verify $((SIDA,T_S),DIDA,S,P)$
Step 2a Calculate $(T_r - T_s)$ and check$(T_r - T_s) > \Delta T$?
Step 3: Now Sensor node B will send its identity with ACK
$((M,SIDB,T_S,S),DIDB)$
Step 4: verify the identity SIDB and check it is already register with BS or not?
Step 4a: Calculate $(T_C - T_S)$ and check$(T_C - T_S) > \Delta T$?
Step 4b: Verify Sensor node B's signature with BS Accept/Reject Signature_Verify
$((SIDB, T_S, DIDB, S, and\ P)$ Step 4c: If all the required identities
are matched, session can be established between the corresponding nodes.

(Fig 1: Authentication Process)


Sensor A
Sensor B
Step 1: SIDA, DIDA
Choose , $r \in Z_q^*$ is a random number from$[1, n-1]$ Compute TSK =
$Hash(Message\ M, Identit\ SIDA)$
(K_{AB}, TSK)
Step 2: Compute shared secret key K_{BA}
Step 4: K_{AB} , S_K
Session Established
ACK (OK message.)
Step 3: Match K_{AB} = K_{BA}?
3.1 if matching, Compute S_K =
$KDF(K_{AB} || T_S)$ $else\ go\ to\ Step 1$.

(Fig 2: Session Establishment Process)

5.2 Security Analysis

To evaluate the security of the proposed protocol SETCTA, we have analyzed various range of security attacks and the protocol can provide strong defense against various adversaries and attacks. Scenarios when a malicious node exists in the network and try to intercept the communication between the sensor nodes.

5.2.1 Node Compromising 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].

5.2.2 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].

5.2.3 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]. Total Size of the message = |SIDAp | + |Ti| + |R| + |V| ranges.

6. EXPERIMENTAL RESULATS

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:

6.1 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.

6.2 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 shown in Figure 4.

6.3 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.

6.4 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:

6.5 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:

Table 2. Message Size Evaluation

Sr No.	Parameters	Description	Size(bytes/bits)
1	$SIDA_{p,}$ p is transmitted packet	Node identity of the transmitted packet p	2 bytes
2	T_S	Sending time-stamp	2 bytes
3	T_C	Current time-stamp	2 bytes
4	R	Message Size	10-15 bytes
5	Key size	ECC over prime field(Fp)	160-bit(20 bytes)
6	V	Variable	Approx. bytes

Table 3. TinyOs Parameters [39]

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 %

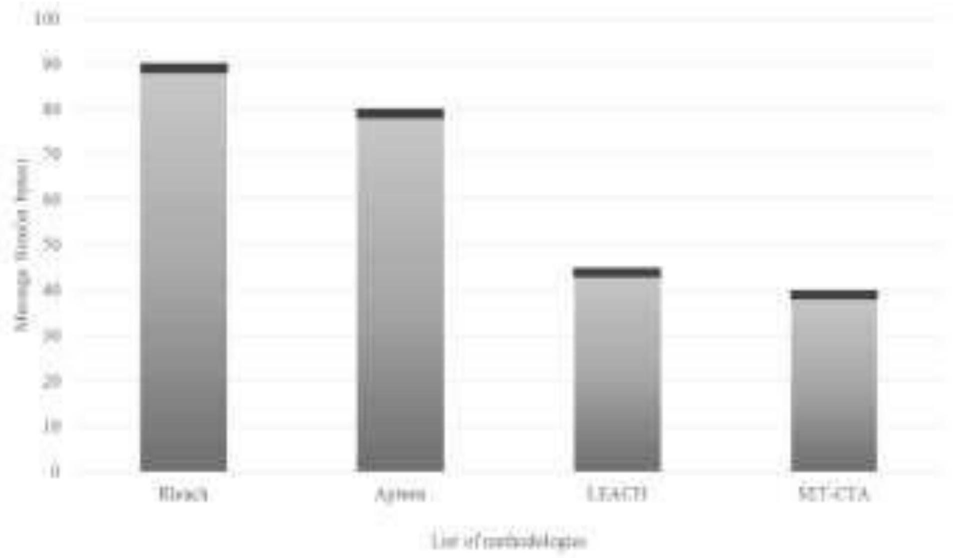


Figure 3. Comparison of Message Size in different security schemes.

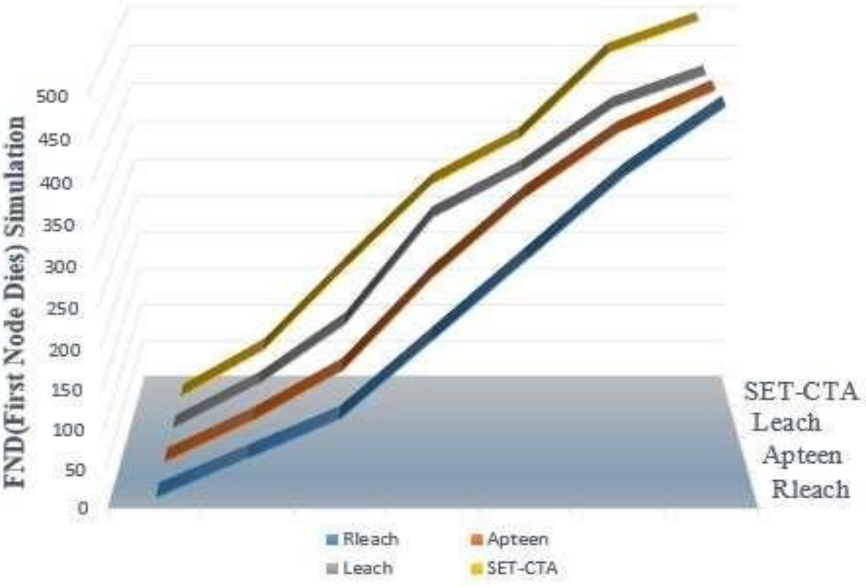


Figure 4. Comparison of FND Time in different security schemes.

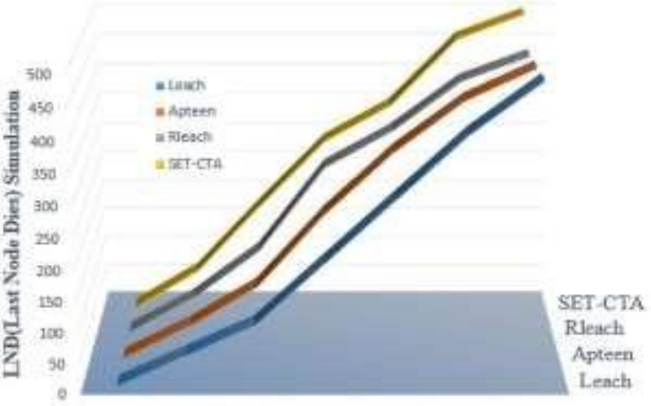


Figure 5. Comparison of LND Time in different security schemes.

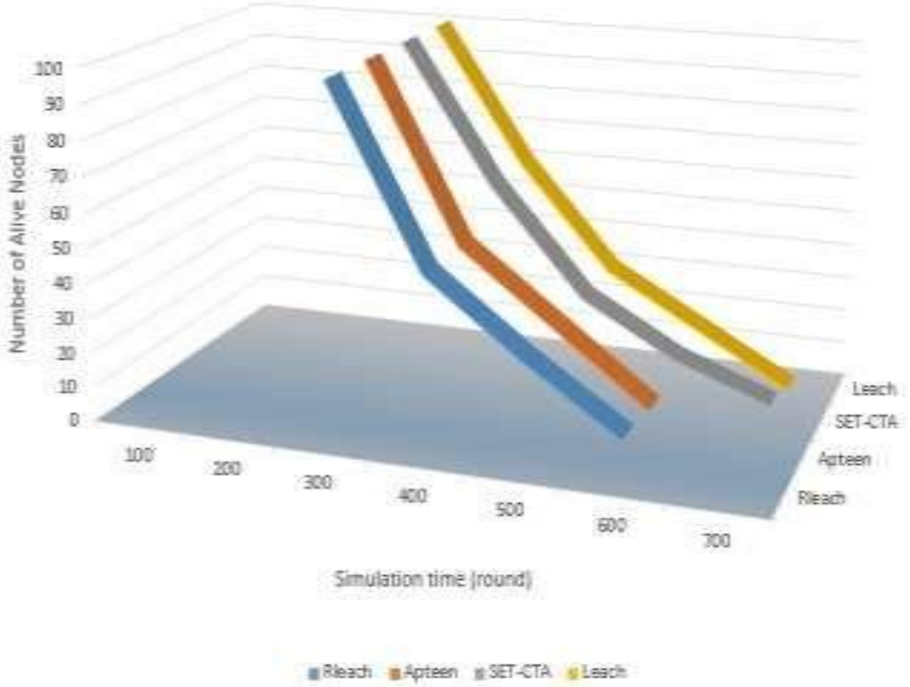


Figure 6. Comparison of Alive Nodes in different security schemes

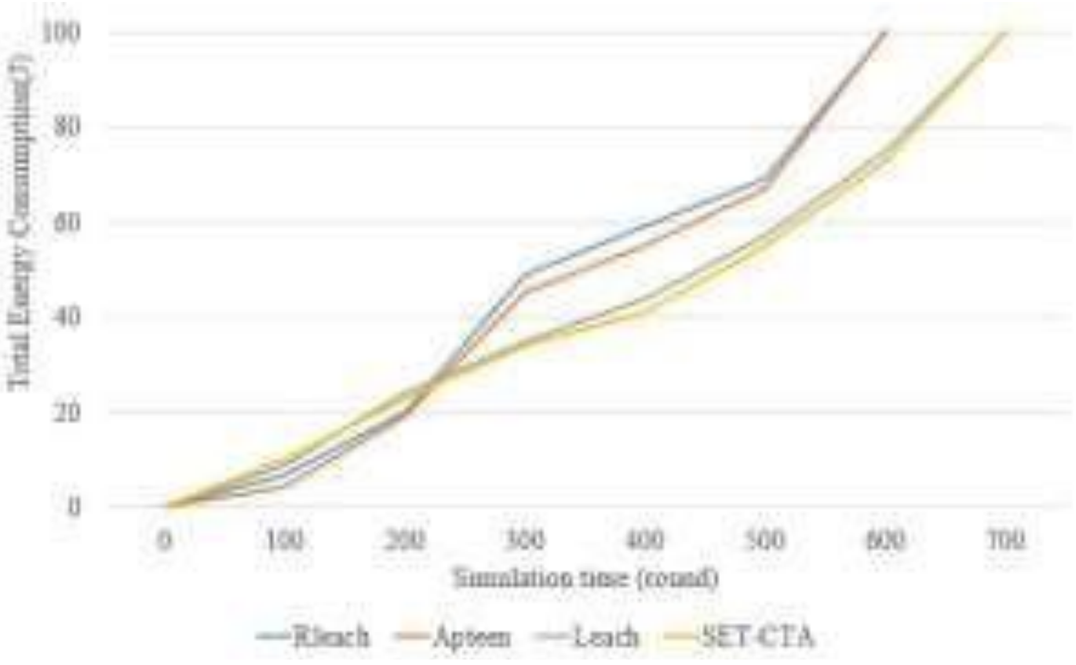


Figure 7. Energy Consumption Analysis

7. CONCLUSION

In this paper, we have traced numerous security challenges, security attacks and analyzed various Leachlike methodologies in centralized wireless sensor environments. We then proposed centralized timestamp based security protocol called “SETCTA”, discussed its characteristics, various passive, active and node compromising attacks. In the evaluation section, we have evaluated the proposed “SET-CTA” protocol against numerous security attacks, security methodologies [XXXXV], communication and computation overhead. We have also provided solutions to provide strong defence against wide range of security attacks by using elliptic curve crypto-system over prime field F_P, concurrency management scheme, timestamp based authentication scheme and session key establishment scheme. At last but not least, we have compared the proposed protocol with the latest research methodologies in terms of transmitted packet size, FND time, LND time, number of alive nodes and energy consumption using various realtime Mica2 sensor kit and simulator results; eventually we have proved that this scheme satisfies high-level security requirements needed in militaries or government organizations and it is also

8. ACKNOWLEDGEMENTS

We are grateful and would like to appreciate efforts of all the people who have helped us directly or indirectly in writing this research paper. Thank you very much for your support and we expect the same in the future.

9. REFERENCES

[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, 2024 June 2011.

[20] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An analytical model for infor- mation 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: Powerefficient and adaptive clustering hierarchy protocol for WSNs," Comput. Commun. vol. 30, no. 14-15, 2007.

[22] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a 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.

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

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

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

[28] 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.

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

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

[31] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing 17:367388, 2007. [2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam.

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

[33] Taekyoung Kwon and Jin Hong, "Secure and Efficient Broadcast Authentica-tion in Wireless Sensor Networks," IEEE Transactions on computers, Vol.59, No.8, August 2010.

[34] 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, 1–10, 2008. 37. Elaine Shi and Adrian Perrig," Designing Secure Sensor Networks," IEEE Wireless Communications, December 2004.

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

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

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

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

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

[40] D. Liu and P. Ning, "Multilevel mTESLA: Broadcast authentication for distributed sensor networks," ACM Trans. Embed. Comput. Syst., vol. 3, no. 4, pp. 800–836, 2004.

[41] 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.

[42]