Authentication Framework against Malicious Attack in Mobile Wireless Sensor Networks

Sunil Gupta, *Member, IAENG*

***Abstract*— Security in mobile wireless sensor networks (MWSNs) is a critical task due to deployment nature and malicious attack. Due to decreasing cost of mobile sensor and increasing capabilities, these networks are used in various applications. The battlefield and health monitoring is the most security oriented field in MWSNs. Security in mobile sensor network has become an important area of research for the network community. Recently, several authentication mechanisms have been proposed against different types of malicious attack in sensor networks. In this paper, an efficient authentication mechanism is proposed to countermeasure the malicious attack in mobile wireless sensor networks. The protocol is well designed for mobile sensor nodes which typically have limited resources. The proposed protocol is based on way hash function and elliptic curve cryptography (ECC). The proposed protocol improves the energy consumption and time taken for access control in comparison with other protocols against various types of security attacks.**

***Index Terms*— Authentication, elliptic curve cryptography, hash function, mobile wireless sensor networks, wireless security.**

I. Introduction

Security is a major concern in MWSNs and it is difficult to implement a security system in a MWSN compared with the conventional desktop computers. Many challenges exist because the sensors restrict the amount of processing power, storage, bandwidth, and energy. These challenges must be overcome because due to importance of security in mobile sensor and its domains that handles sensitive information. Therefore, many factors must be investigated properly for protecting the sensitive information transmitted between nodes (which can be mobile sensor nodes or the BS) from being intruder to third parties [1].

Confidentiality is a property of the WSN for security. In the absence of security, an application domain leads to undesirable consequences. WSNs are rapidly gaining popularity because of their low-cost solutions to the various real-world challenges [1]. Mobile sensor network used presently can monitor humidity, pressure, temperature, soil makeup, vehicular movement, noise levels, lighting conditions, absence or presence of definite types of matters, mechanical stress levels in involved matters, and other possessions. Wireless transceivers are used for communication between sensors in MWSNs.

Although advances toward counteracting potential threats in sensor networks are observed, these security measures are inadequate [1]. Practically, a major challenge in employing an efficient security scheme in MWSNs is the size of the sensor network. For addressing security issues in MWSNs, we focused on steganography, cryptography, and other network security basics and their uses. We explored different types of threats and attacks that may harm MWSN functioning. For reducing the manufacturing cost, a mobile sensor node is built as a tiny device. Therefore, to design a security solution, we must focus on resource constraints, such as limited memory, limited energy, limited computational power, limited communication bandwidth, and limited communication range. Capabilities and mobile sensor node hardware constraints act as a dependent platform for the type of security mechanism that can be hosted on a sensor node platform. Because of the uneven distribution of the traffic load, some network nodes may lose their power after several weeks or months. Therefore, deploying new nodes is essential in this case. In addition to the natural loss of mobile sensor nodes, it is susceptible to malicious attacks in hostile and unattended environments.

Some nodes may be destroyed by attackers to make the entire network inoperative. Thus, new mobile sensor nodes must be deployed. However, an attacker can add malicious nodes in the network, leading to message eavesdropping and insertion of false reports.

We observed that malicious attacks manipulate the existing nodes to introduce malicious “new” nodes, which are indistinguishable from legitimate new nodes in the current sensor network security technology. These new malicious nodes could be accepted as legitimate ones by the other normal nodes. Therefore, we present a new framework for sensor networks in order to prevent malicious nodes. However, previously proposed key predistribution schemes are difficult to implement as a dynamic access control because all old secret keys and broadcasting messages of the existing node must be updated when a new node is added [2].

II. Salient features of security

A. Cryptography

The cryptography methods developed for the traditional wired networks are not feasible to be directly applied for mobile wireless sensor networks. Applying the encryption could also increase the delay and require transmission of extra bits [3]. Furthermore, problem is arise when applying

Dr Sunil Gupta is currently working as Associate Professor in the Department of Computer Science and Engineering at BML Munjal University, Gurgaon, India. (E-mail: sunil.gupta@bml.edu.in).

encryption schemes to MWSNs like, key management, addition of new sensor node or renewed for ensuring robust security for the mobile sensor network [4].

B. Steganography

A Steganography aim is to hide the existence of the message. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing mobile wireless sensor networks is not directly related to steganography and processing data [4].

C. Need for authentication protocol

Because of open communication channels, MWSNs can be affected by many security threats, therefore, only authorized nodes must have access to information. A sensor node platform is dependent on the constraints and capabilities of mobile sensor node hardware. After operating for several weeks or months, some nodes in the network may lose their power because of the uneven distribution of the traffic load; therefore, a new node must be deployed. Moreover, because of the natural loss of mobile sensor nodes, a sensor node is vulnerable to malicious attacks in a hostile and unattended environment. The adversaries destroy the nodes, making the entire network inoperative. Therefore, new mobile sensor nodes are essential to positioning. However, an opponent can also deploy malicious nodes in a network. These malicious nodes may easily eavesdrop messages or insert false reports.

.

III. Related Work

In the deployment of MWSNs, security is actually a critical problem. Several researchers have attempted for securing sensor networks.

Cheng et al. [5] proposed a new access control method based on elliptic curve cryptography and the chameleon hash function. This method based on the chameleon hash function and used twice Diffie-Hellman key exchange. This method used signature parameter to archive robust authentication and key exchange. In the authentication and key establishment phase, node authenticates node based on the chameleon hash value of the node. All nodes of the WSN have the same chameleon hash value as the base station. The proposed method can resist attacks such as legal node masquerading attacks, forgery attacks, new node masquerading attacks, replay attacks, and man-in-the-middle attacks.

Zhi et al. [6], the key idea was that the gateway node (GW- node) allots different secret keys to each user ID and each sensor node to avoid GW-node impersonation and GW-node by passing attacks. The authors assumed that the user ID cannot impersonate the GW-node without its secret key. Therefore, it is difficult for the opponent owning one sensor node secret key to bypass the GW-node for accessing other sensor nodes without their corresponding secret keys. Their proposed scheme comprises of includes three phases: registration, password change, and authentication. In the registration phase, the GW-node generates an initial password for the user ID. This design not only well adapts to the style of the card issuer but also thwarts the privileged-insider attack. After receiving the smart card, users can immediately change the initial password by using the password change operation. In the password change phase, users can freely change their password without any interaction with the GW-node. Because the GW-node cannot modify any user’s password information, this design prevents the possibility of the privileged-insider attack. The authentication phase is invoked when the user wants to perform some query or access data from the WSN. The authors related the proposed protocol only with the scheme by [Khan et al., 2010] because both the schemes were based on the same encryption tool and provided the same security goals. The proposed scheme differs in terms of nonce, whereas the scheme by Khan et al. is based on a timestamp. For timestamp-based systems, time clocks should be both secured and synchronized. The prevention of the adversarial modification of local time clocks is difficult to guarantee in many distributed systems, for example, WSNs. As a disadvantage, the nonce-based system needs one additional message exchange compared with the timestamp-based system.

The authors highlighted two areas for the future studies. First, an appropriate formal model for examining the security of the user authentication scheme for WSNs; second, the method for presenting a formal definition of the user authentication under the WSN setting and designing the scheme, which can be reduced to satisfy the definition assuming minimal cryptographic algorithms.

Arikumar et al. [7] introduced an improved user authentication method for WSNs. According to this method, the user receives a smart card from the GW-node during the registration phase, and then the user password and smart card allow the user to log in to the sensor/GW node for accessing the data in the network. This scheme involves three phases, namely, the registration phase, authentication phase, and password change phase.

Once the registration phase is completed, the authentication phase is performed each time the user logs into the system. This protocol escapes many logged-in users with the same login ID and stolen-verifier attacks; these are projecting threats for a password-based system if it keeps the verifier table at the GW-node or sensor node. In addition, this protocol resists other attacks in WSNs except the node compromise and DOS attacks. This protocol allows the users to select and change their passwords easily. This system is well-designed for WSNs with limited resources to authenticate without the public key requirement, and it uses only smart cards and one-way hash functions and can be efficiently implemented.

Yeh et al.[8] proposed a secured authentication protocol for WSNs using ECC and their analysis, with a comprehensive analysis of the protocol proposed by [Das, 2009], and showed some security pitfalls of the protocol. In addition, the authors proposed a more efficient authentication protocol using ECC. They revised the basics of ECC; therefore, the proposed protocol is suitable for secure authentication in WSNs. The protocol consists of five phases: registration, login, verification, mutual authentication, and password changing.

The authors discussed the security issues of remote user authentication, which includes resistance to masquerade and insider attacks, mutual authentication, and securely changing or updating a password. They stated that the protocol proposed by wong[9] in year 2000 which is not suitable for mutual authentication because it is vulnerable to replay and forgery attacks.

The calculation is performed by combining point multiplication and addition. The authors considered that the ECC computational cost for generating a small key size is lower than RSA security. The ECC-based protocol is more useful than another protocol because it resolves the weaknesses of the other protocol and is suitable for many applications demanding a high security. The proposed protocol resolves the issue of mutual authentication observed in the protocol proposed by Das and uses less hash function compared with the other protocols. The authors presented a comparison of computation and communication costs, security, and performances of the proposed protocols.

Vaidya et al. [12] suggested an improved two-factor user authentication in WSNs. This new scheme can overcome the drawbacks of the schemes proposed by Khan–Algahathbar and Das and can provide strength and security at higher levels. The scheme proposed by Das specified that WSNs are positioned in a limited area, which could be separated into different zones. Authorized users can access a WSN by using their mobile devices (e.g., PDA and notebook). For accessing a sensor node, the user must first register with the GW-node, and after a successful registration, the query is sent by the user to a wireless sensor node in a predefined configuration period. The basic idea of the protocol is that during the registration phase, a user receives a smart card from the GW-node. Furthermore, during the login–authentication phase, the main goal is to reduce the potential problems caused by illegitimate users and compromised smart cards. Thus, the authors proposed a smart card-based password user authentication scheme to fulfill the following requirements:

- It defends against various attacks based on the use of a stolen smart card.
- The scheme provides mutual authentication between the SN- and GW-nodes to remove the forgery attacks.
- The proposed protocol is lightweight and efficient for computation and communication.
- The scheme is based on the zero-knowledge-based password protocol, which means that it allows an applicant to authenticate to a verifier without revealing the user password.
- The scheme facilitates changing the password and update other constraints.

Daojing et al. [9] proposed an enhanced scheme by preserving the merits of the original protocol. In addition, they observed a drawback of the original scheme [Das, 2009] that a user cannot change a password securely and easily. To eliminate this drawback, the password updating phase was added. The enhanced scheme includes three phases: registration, authentication, and password updating.

This proposed scheme is an enhancement of the previous scheme [10], which preserves the merits of the original scheme. This scheme can resist stolen-verifier and guessing attacks because the user password is not transmitted simply as the hash of the password. In addition, a timestamp is used to prevent the replay attack. Moreover, the proposed scheme can overcome the security flaws of the original scheme [10]. The advantages of the proposed scheme can withstand the insider attack, and the impersonation attack can obtain a user's real identity.

Khan et al. [11] proposed cryptanalysis and security improvements of the two-factor user authentication protocol for WSNs. The authors showed that the previous scheme [10] had some pitfalls and cannot be applied for real-time applications. They found that the scheme proposed by Das does not allow the users to change and update their passwords, provide the mutual authentication between the sensor and GW-nodes, and prevent the insider and GW-nodes by passing attacks. To overcome the essential security pitfalls of this aforementioned scheme, the authors recommended enhancements and security covers that attempt to fix the vulnerabilities of this scheme.

The authors stated that the protocol cannot share the secret parameter with others and a sensor node, and each entity has its own secret key or parameter. Furthermore, they suggested that the GW-node should only share the user ID with a sensor node and another secret key must be present, which should only be known to the sensor nodes and GW-nodes; before deployment, it can be stored in the sensor nodes. These sensor nodes are responsible for responding to the user inquiries.

Although in a projected security cover, an overview of another secret parameter creates storage overhead on the GW-node; however, it provides benefits and cannot be overlooked. The benefits are that it protects the GW-node from a passing attack and it is easy to update the secret key when compromising secret parameters by an adversary.

This scheme is advantageous as it defends against the insider attack, provides a password updating and changing option, protects GW-nodes from the passing attack, and achieves mutual authentication between GW- and sensor nodes, which require slightly more hashing operations than those required to increase the security of the complete authentication scheme. Hence, the computational overhead is not extremely high for the proposed scheme; however, the system covers some enhanced features of security.

IV. WEAKNESS OF PREVIOUS PROTOCOL

Recently, many schemes have been proposed [5-8] to protect sensor networks; however, some weaknesses remain in them. These schemes may prevent attackers from eavesdropping messages or inserting false reports. However, they cannot provide a better authentication protocol that can defend against internal attacks in mobile sensor networks. Following are some weaknesses of previous protocols [5-8].

- Previous protocols provide one-way authentication only, thereby not ensuring consistency/session key freshness for enhancing sensor node security.
- An intruder can easily obtain the key for authentication.

- Unauthorized users can access services.
- The problem of eavesdropping attacks
- High-cost security
- The suggested protocols are not beneficial because they lack mutual authentication.

V. Proposed Protocol

The proposed protocol uses a cryptographic tool, including ECC with the Diffie–Hellman scheme because ECC can attain the highest level of security with reduced key sizes, and DSA for verifing the signature. We know that 160- and 224-bit ECC provide comparable security to 1024-bit RSA and 2048-bit RSA, respectively. With the same level of security, smaller key sizes of ECC offer faster computation. The proposed protocol composed of predeployment, registration, login and authentication phase.

A. *Predeployment phase*

Before a mobile sensor network is deployed, the base station chooses a set of system constraints that includes:
1. A finite field Fq, where q is at least 160 bits of a large odd prime.
2. An elliptic curve E over Fq Ep (a, b)—an elliptic curve with a parameter a, b and p are prime number.
3. G is a cyclic group point on an elliptic curve with a high order value n, at least 160 bits.
4. The base station's private key k = {1, 2, 3………, n−1}.
5. The base station's public key Q = kG; the base station shares its private key with anyone else.

B. *Registration phase*

In the registration phase, the user Ui registers itself with a MWSN through the following steps:
1. A user Ui must submit its identification IDi to the base station/gateway over a secure channel.
2. The base station/gateway confirms IDi after receiving the registration request from a user Ui and generates Vi = h[(IDi||K)||h(Pwi)]. The base station generates the values of the hash function and then stores them on a system.
3. The base station/gateway provides a token/smart card and password (Pwi) to the user through a secure channel.
The initial password is supplied by the gateway node, making this scheme unprotected from the privileged-insider attack. It is recommended that once a user Ui receives the token/ smart card. Figure 1 shows the state transition diagram of the registration phase.

A. *Login phase*

When a user Ui wants to access data or perform some query for MWSNs, then a user Ui first needs to login. The steps of the login phase are as follows:
1. If a user Ui wants to perform a query, then the user Ui has to provide the user IDi and password Pwi to the gateway. First, user Ui send a token in the gateway. Then, the user sends IDi and Pwi, and then the token/smart card verifies the entered values with the stored values; if both the values match, the token generates a Hello packet to the gateway node. If one of the values does not match with the stored value, then the login request is rejected.
2. After receiving the Hello packet from the user Ui, gateway node generates nonce N1 and sends it to the user.
3. After receiving N1 from the gateway, the smart card calculates the identities
Ai = h[ViXOR h(Pwi)]||N1 and h(S||T).
Here, S is the secret key and T is the timestamp.
Subsequently, the token sends IDi, Ai, and h(K||T) to the gateway node.
4. After receiving Ai, IDi, and h(K||T), the base station verifies the validity of time with ΔT = T2 − T1; if it is valid, then it checks A = h1[h(IDi||K)||N1] using the secret key S. The user Ui request login is rejected if either of IDi or Ai is invalid and the session is terminated. Otherwise, the base station accepts the user Ui login request. Figure 2 shows login phase.

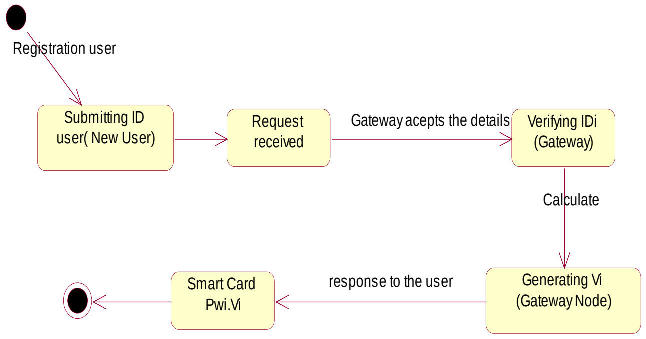

Figure 1: Registration phase state transition diagram

A. *Authentication phase*

After the login phase, the base station generates nonce N2, and then sends a message with the identification and same nonce {IDi, N2} to an adjacent mobile sensor node (MSN) over a public channel for responding to a query or accessing data, which a user Ui is looking for.
1. On receiving the message with identification and nonce {IDi, N2}, the selected MSN generates nonce N3 and calculates Bi = h[h(SIDn||K)||IDi||N2||N3] using the secret key h(SIDn||K). MSN then sends the message {SIDn, Bi, N3} to the base station.
2. On receiving the message {SIDn, Bi, N3} from Sn, the base station verifies the validity of SIDn and BS = h(h(SIDn||K)||IDi||N2||N3) using the secret key S. If the verification fails, the base station terminates the session. Otherwise, it calculates the value
Ci = h1[IDi||h(SIDn||K)||N3||N2] and sends back a mutual authentication message {Ci} to MSN.
3.On receiving the message {Ci}, Sn verifies whether
Ci = h1[IDi||h(SIDn||K)||N3||N2] is valid. If the certificate Ci is unacceptable, MSN ends the session; otherwise, Sn sends a successful signal to the base station.
4.On receiving the signal, the base station sends a favorable message to the user Ui, and the session is effective. Figure 3 shows a user authentication session for a node.

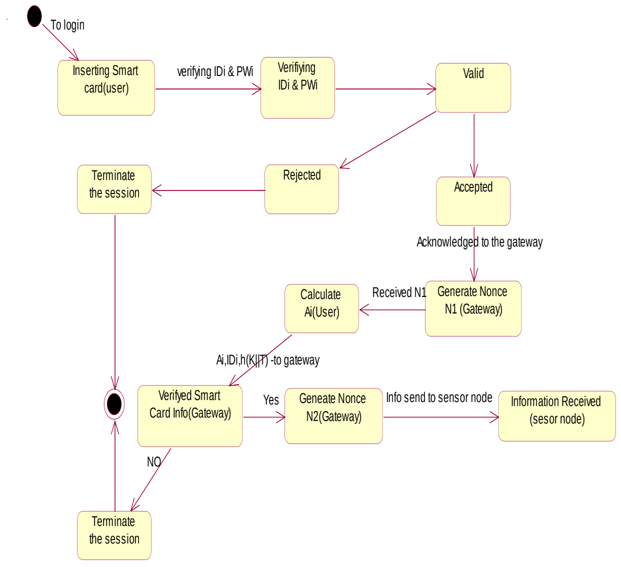
To login
Inserting Smart card(user)
verifying IDi & PWi
Verifying IDi & PWi
Valid
Rejected
Terminate the session
Accepted
Acknowledged to the gateway
Generate Nonce N1 (Gateway)
Received N1
Calculate Ai(User)
Ai,IDi,h(K||T) -to gateway
Verifyed Smart Card Info(Gateway)
Yes
Geneate Nonce N2(Gateway)
Info send to sensor node
Information Received (sesor node)
NO
Terminate the session

Figure 2: Login phase transition diagram

.

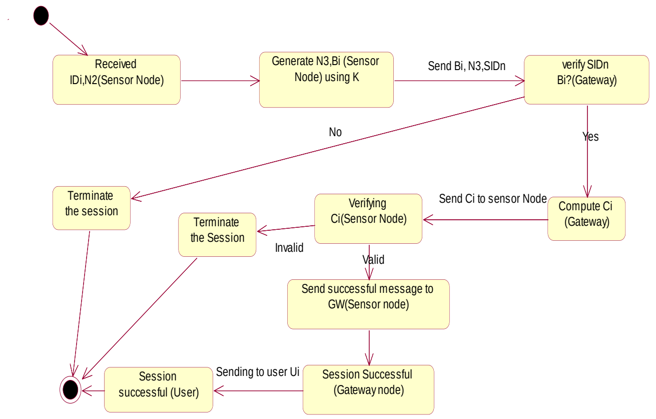
Received IDi,N2(Sensor Node)
Generate N3,Bi (Sensor Node) using K
Send Bi, N3,SIDn
verify SIDn Bi?(Gateway)
No
Yes
Terminate the session
Terminate the Session
Invalid
Verifying Ci(Sensor Node)
Send Ci to sensor Node
Compute Ci (Gateway)
Valid
Send successful message to GW(Sensor node)
Session successful (User)
Sending to user Ui
Session Successful (Gateway node)

Figure 3: Authentication phase transition diagram

VI. Performance Evaluation

Computational Cost: This paper evaluates the price of security in terms of execution time and energy overhead for each operation at the mobile sensor node. Table I shows security prices at each mobile sensor node. According to practical implementation on MICA2 motes the computational time for performing T_H (one hash function) is 3.636 ms, and time for performing T_{XOR} (exclusive-OR) function is 4.143 ms [13].

The proposed protocol takes less time ie approx. 46ms in comparison with other related protocol. Figure 4 shows the comparison of total number of hash function, exclusive-Or and total delay occurs in protocols. It shows significant improvement in proposed protocol.

TABLE I: COMPUTATIONAL COST COMPARISON

Phase	Daojing He	Khan-Algahathour	Binod Vaidya	Proposed Protocol
Total Cost	$17T_H+12T_{XOR}+4C_{MH}$	$18T_H+11T_{XOR}+4C_{MH}$	$24T_H+15T_{XOR}+4C_{MH}$	$10T_H+3T_{XOR}+4C_{MH}$
Total Time Taken	111.528 ms	111.021 ms	142.857 ms	46.059 ms
Total Energy consumption	2.676 mJ	2.66 mJ	3.42 mJ	1.10 mJ

The energy consumption of each operation can be estimated using the formula E = U * I * t , where U is the voltage , I is the current in active mode and t is the execution time for MICA 2 mote, when a processor is in active mode I= 8mA and U= 3.0 V if two new AA batteries are used.

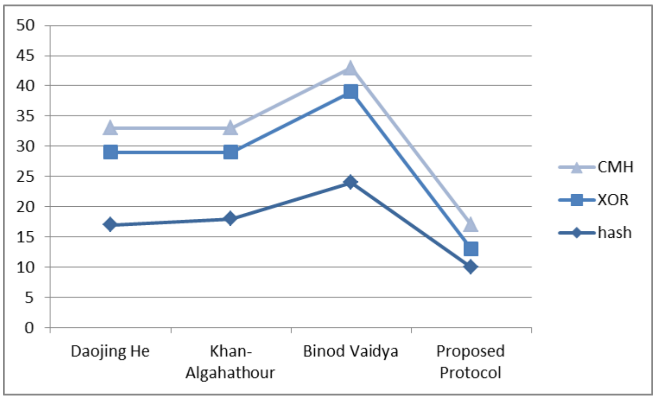

Figure 4: Total computational cost

Figure 5 and Figure 6 shows the total time required and energy consumption for each protocol. the figure shows that the proposed protocol consume less energy and time in comparison with other protocol.

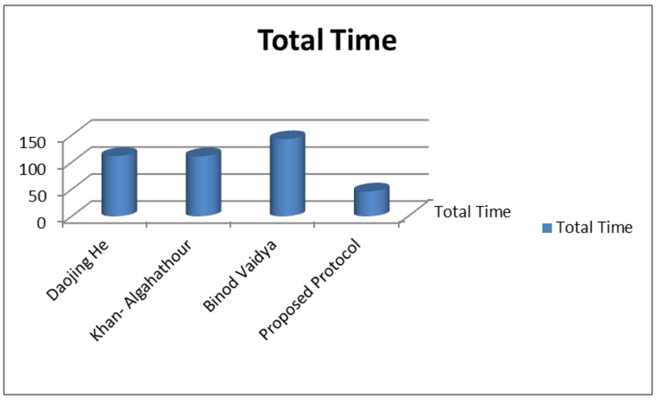

Figure 5: Total time taken

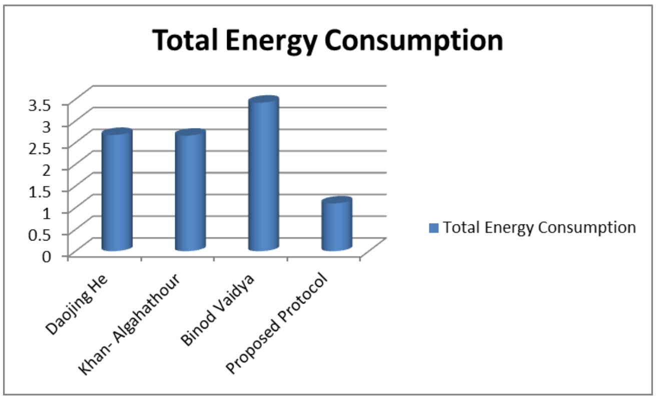

Figure 6: Total energy consumption

The proposed protocol takes less consumption of energy i.e. 1.10 mJ, and its less than other related protocols.

VII. Conclusion

In this paper, author proposed an authentication protocol by using elliptic curve cryptography to communicate a user to mobile sensor network. The authentication protocol can avoid malicious nodes from joining sensor networks at establishment of network. In adding up, key establishment by using elliptic curve is also realized in our protocol to help the new node establish shared keys with its neighbors so that it can perform secure communications with better key management Compared with the RSA, DH, DSA our protocol with ECC can protect against most of the infamous attacks in sensor networks, and achieve better communication and computation performance.

This study and proposed scheme of authentication in mobile wireless sensor networks gives a broad view for researchers on how to make an authentication scheme which provide security measure with computational cost and its overhead. In this paper, author discussed different authentication protocols that removes the vulnerabilities and provides robust security against malicious attacks in communications of mobile wireless sensor networks.

References

[1] Tanweer, and A.Y. Zomaya, "*A security framework for wireless sensor networks*", Proceedings of IEEE sensor applications symposium, February, pp.89-97, 2006.

[2] Holohan, E., "*Authentication using virtual certificate authorities: a new security paradigm for wireless sensor networks*", Proceeding of network computing and applications , July, pp. 92-99, 2010.

[3] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar,"*SPINS: security protocols for sensor networks*", Proceedings of wireless networks journal (WINE), September, pp. 78-89, 2002.

[4] Kaplantzis, S., "*Classification techniques for network intrusion detection*", tech. Rep., Monash University, ECSE, October, pp. 335-342, 2004.

[5] Cheng, Y., Alan, D., and Wang, H., "*Secure access control method for wireless sensor networks*", International Journal of distributed sensor networks, Vol 2015, no.1, pp. 1-6, 2014.

[6] Zhi, S., Jian-Xin, L., Zhi-Yong, F., Zhen-Fu, C. and Guang-Quan, X. , "*On the security and improvement of a two-factor user authentication scheme in wireless sensor network*", Vol. 17, no.5 pp. 895-905, 2013.

[7] Arikumar, K.S. and Thirumoorthy, K., "*Improved user authentication in wireless sensor networks*", Proceeding of ICETECT, March, pp.1010-1015, 2011.

[8] Yeh, H.L., Chen, T.H., Liu, P., Kim, T.H. and Wei, H.W. "*A secured authentication protocol for wireless sensor networks using elliptic curves cryptography*", Sensors, Vol.11, no.5, pp.4767-4779, 2011.

[9] Daojing, H., Yi, G., Sammy, C., Chun, C. and Jiajun, B., "*An enhanced two-factor user authentication scheme in wireless sensor networks*", Adhoc & sensor wireless networks, Vol.10, no.4, pp.361–371, 2010.

[10] Das, M.L.,"*Two-factor user authentication in wireless sensor networks*," IEEE transactions on wireless communications, Vol. 8, no. 3, pp.1086-1090, 2009.

[11] Khan, M. K. and Alghathbar, K. , "*Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks*'", Sensors , Vol. 10, no.3, pp. 2450-2459, 2010.

[12] Vaidya, B., Makrakis, D., and Hussein, T., "Improved two-factor user authentication in wireless sensor networks", Second IEEE international workshop on network assurance and security services in ubiquitous environments ,October, pp. 600-606, 2010.

[13] N. Gura, A. Patel, A. S. Wander, H. Eberle, and S. Chang Shantz, "*Comparing elliptic curve cryptography and RSA on 8-bit CPUs*", in Cryptographic Hardware and Embedded Systems — CHES 2004, vol. 3156 of Lecture Notes in Computer Science, pp. 119–132. Springer Verlag, 2004.

Dr Sunil Gupta is currently working as Associate Professor in the Department of Computer Science and Engineering at BML Munjal University, Gurgaon, India. He has done his Bachelor's degree in Computer Science and Engineering and Master's degree in computer science and engineering from National Institute of Technology Hamirpur. and Ph.D. from National Institute of Technology, Jalandhar India. He is presently working in the area of Information Security, Computer Networks and Scientific Computing. He has many publications of international /national level to his credit. (E-mail: sunil.gupta@bml.edu.in).