An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC

Rakesh Maharana
Department of Computer Science & Engineering
National Institute of Technology, Rourkela, India

Pabitra Mohan Khilar
Department of Computer Science & Engineering
National Institute of Technology, Rourkela, India

ABSTRACT

User authentication in case of wireless sensor network is a very critical task, as sensor nodes are deployed in unattached environment and are prone to possible hostile network attacks. Any authentication protocol in WSN must be designed keeping the fact that sensor nodes have limited computing power, memory, energy and communication capabilities. In this paper,animproved user authentication protocol based on Elliptic Curve Cryptography (ECC) has been introduced for hierarchical wireless sensor networks (HWSN). This paper shows that the ECC based protocol is suitable for wireless sensor networks where higher security is demanded. Besides thisthe proposed scheme provides mutual authentication and a secret session key for communication between the user and the cluster head. It also providesan option for addition or replacement of cluster head in the network whenever there is a need.

General Terms

Wireless sensor networks, Security.

Keywords

User Authentication; Security; Public Key Cryptography (PKC); ECC; Smart Card; Hierarchical Wireless Sensor Network (HWSN).

1. INTRODUCTION

In a wireless sensor network (WSN), huge numbers of sensor nodes are deployed in the target field. After their deployment, the sensor nodes form ad-hoc infrastructure-less wireless network. Then these nodes communicate with each other using wireless communication within their communication range. Those sensor nodes gather environmental data and transferred those data to a single point called Base station or Gateway node (GW node). Here data are routed to the base station via the multi-hop communication path. These sensor nodes are easy to deploy. They can be dropped on a particular area from the truck or plane and then each sensor node coordinates with their neighboring sensor nodes and together these nodes form a network which finally linked to base station [1]. These tiny sensors have limited energy, low processing power and less memory. But they play a very important role in various areas like real-time traffic monitoring, military sensing and tracking, building safety monitoring, measurement of seismic activity, wildlife monitoring and so on. When user wants some data he/she puts a query to the GW node or Base station and GW node gives data collected from the sensor node. But consider the situation like battle field where users are in the deployed area and they need real-time data. In those situations if they collect data from the GW node the data may not be real-time as there is always transmission delay or periodic nature of data collection. In those cases the appropriate decision cannot be taken quickly and correctly. So they need to collect data from the sensor node directly. If the data in the wireless sensor network are made available to users on demand, then authentication of user must be ensured before allowing the user to access data.

A proper user authentication scheme in wireless sensor network is difficult task. The main problem for this is resource-constraint nature of the WSN. That means sensor nodes have very limited energy, computing power and memory. As cryptographic concepts like public key cryptography take more computing power and require more energy, their use is avoided here. But the use of PKC based on elliptic curve cryptography is feasible in case of wireless sensor network [2], [3]. Comparing RSA and ECC, it is found that RSA is based on integer factorization and the best algorithm to solve this integer factorization is sub-exponential whereas the best algorithm to solve ECC is exponential [3]. That's why compare to RSA, ECC can provide the same level of security with smaller key. ECC of key length 160 bits gives the same level of security as RSA of 1024 bits key length [3]. This difference in length also affects the performance. So RSA consumes more energy than ECC [4]. As in case of WSN there is limited energy, computational power and memory so, ECC is preferred.

Here a smart-card based user authentication scheme in hierarchical wireless sensor network using ECC is proposed. This scheme combines ECDH and cryptographic hash function to provide authentication as well as a session key for further communication between user and cluster head.

Organization of the paper

The rest of this paper is organized as follows. In Section 2, network model is described. In section 3, existing works on user authentication in WSNs. Section 4 gives the overview of ECC and in section 5 describesa secure authentication protocol for HWSNs using elliptic curve cryptography. Section 6 describes security analysis of proposed scheme and shows the performance comparison with related scheme. Section 6 concludes the paper.

2. NETWORK MODEL

In traditional WSN, there is a trusted base station which is responsible for collecting data from the sensor nodes and also responsible for processing requests from the users. Here the sensor nodes have very limited energy, computing power and less memory storage. These sensor nodes also have a low transmission range. This architecture performs smoothly for small networks.

For larger networks hierarchical wireless sensor network [23] (HWSN) is preferred. In this type of network there is a hierarchy which is based on their capabilities. i.e. sensor node, cluster head and base station from lower to higher level.

Sensor node: These nodes are the generic sensor node. These nodes have very limited energy, computing power and short transmission range. In a cluster these nodes communicate with the cluster head of that cluster. These nodes do the actual sensing job and then share the information with the cluster head.

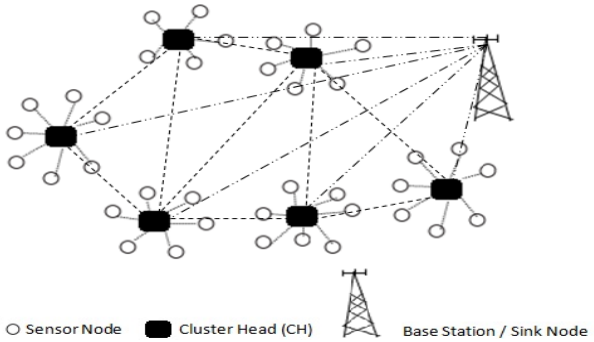

Fig 1. A hierarchical wireless sensor network model [23]

Cluster head: These are special type of nodes which have more resources than generic sensor nodes. They have more energy, computing power, memory storage and also a higher transmission range. These cluster heads collect data from the sensor nodes in its cluster and communicate those data with other cluster heads as well as with base station. As they have the higher computing power, they can process complicated computing operations.

Base station: This is a powerful node having a wide communication range. The base station is not limited by energy, computing power or memory. It is also an access point for human interaction.

There are so many advantages of using HWSN. The cluster structure of HWSN makes it stable. If user wants to know the information for a particular area it can get from the cluster head within that area directly. It makes the sensor nodes more efficient as they are not involved in transmission and user query processing. It also helps in eliminating redundant data. It improves network life time and also reduces network traffic and contention. The main advantage of this architecture is, cluster heads have more computing power and energy powerful security protocol can be integrated.

3. RELATED WORK

In this section, a brief discussion of the existing user authentication schemes in wireless sensor network is given.

Watro et al. [7] proposed a user authentication scheme for WSN called TinyPK which is based on PKC. Here it uses RSA [5] and Diffie Hellman protocol [6]. This protocol suffers from the "masquerade as sensor node to an unknowing user" attack [15]. After receiving the user's public key, the intruder encrypts a session key and other parameters. Then it sends it to the user. The user believes that the message has come from the sensor node. It decrypts the message with the private key and uses the session key for further communication. This scheme also computationally inefficient and does not provide mutual authentication.

Benenson et al. [8] mentioned several security issues in WSN, specifically the access control and proposed a method where the user can successfully authenticate with any subset of n sensors. Then Benenson et al. [9] proposed another solution which based on Elliptic Curve Cryptography. In this scheme sensor nodes require high storage space as each pair of node requires a secret key. Here all user queries are processed by a single node. This node should be identified while authentication. But in Benenson's scheme there is no procedure given to find that node. This process also requires each node to know the entire network. There is no provision to deal with the situation where the node responsible for process the query is compromised and sends false information.

Wong et al. [10] proposed an efficient user authentication scheme. It is based on user's password and uses cryptographic hash function. It has security flaws like many logged in users with same login-Id threat in which if an attacker has a valid user's password, he/she can login to the sensor network. It also suffers from stolen-verifier attack as both GW-node and login-node keeps the lookup table of registered user's secret information.

Banerjee et al. [11] proposed a fully symmetric key based scheme for authenticating user in WSN. Here any node can reply to the user's query. It uses the pairwise key pre-distribution scheme proposed by Blundo et al. [12]. Here the node which process user's query generates a nonce and user must calculate a valid MAC for the generated nonce and sends back this MAC to the node. If the sensor does not receive a valid MAC, then it discards the login request. This scheme does not provide mutual authentication and prone to node compromise attack. It does not give clues how to find sensor node which will process the user's query.

Jiang et al. [13] proposed a distributed user authentication scheme in WSN. It is based on self-certified cryptosystem (SCK) which is modified to use ECC to establish pairwise keys in sensor networks. Here the nodes which are in the transmission range of user, act collaboratively to find out whether the user is allowed to access the sensor network or not. The drawback of this scheme is that each node which receives the access request of the user has to compute a pairwise key which will be shared with the user. It also uses an encrypted nonce using ECC which is an expensive task for sensor node.

Tseng et al. [14] proposed a user authentication scheme which is an improved version of Wong et al. [10] scheme. It is resistance to reply attack and forgery attack and also allows user to change his/her password freely. It also allows user to login from any sensor node in the network. After receiving login request from user sensor node forward this request to GW-node which verifies authenticity of the user. User registration is performed at the GW - node. The weakness of scheme is, it cannot resist node compromise attack and it requires time synchronization but nodes which is difficult task in case of WSN.

Das [15] proposed a two-factor user authentication scheme in wireless sensor network. He mentioned security vulnerabilities in Wong et al. [10] scheme like many logged-in users with same login-Id threat and stolen verifier attack as GW-node and login-node maintains a lookup table of the entire registered user's secret information. He proposed protocol to overcome the security flaws of Wong et al. [10] scheme. He used a two factor user authentication scheme based on a smart card and password. However it cannot solve the problem like DOS attack and node compromise attack. Here user cannot freely and securely change his/her password.

Another problem is time synchronization as it uses the time stamp to restrict replay attack.

Khan and Alghathbar [16] showed that ML. Das scheme is not secure against gateway-node bypass attack, does not provide mutual authentication and also vulnerable to privileged insider attack. They also showed that ML. Das scheme does not have provision to change password. They proposed a scheme which overcomes those security flaws.

He et al. [17] proposed an improved scheme based on ML. Das scheme. It keeps all the merit of the ML. Das scheme and provides protocols to restrict insider attack and impersonation attack and provides methods to update the password.

Cheikhrouhou et al. [18] proposed a light weight user authentication scheme for wireless sensor networks. Here user uses a PDA to authenticate himself/herself. It uses AES for encryption and decryption. In this proposed scheme administrator chooses a secret key x and load it in the system server and coordinator node. This secret x is used by the system server for registering the users. The coordinator uses this secret to verify the authenticity of users. Here a secret S is computed using secret $x$by the coordinator node. Here the problem is, if coordinator node is compromised, all secret values of users will be known to the intruder which will create a valid ID and a secret value S.

In 2010 Tseng et al. [19] proposed a robust user authentication scheme for wireless sensor network based on elliptic curve crypto-system with self-certificates. In this scheme KDC is responsible for initialing system parameters, generating identity, generating private/public key-pair and distributing the certificate to each user and each sensor node. The problem is users and sensor nodes have to store a lot of parameters. Here the user's identity is verified by the sensor node by checking the signature using Elliptic Curve which is a costly task. It also suffers from DOS attack. Here by sending invalid certificates or invalid signature to the sensor node the attacker can exhaust the memory at the node or make the node running out of energy.

Kumar et al. [20] proposed an efficient two-factor user authentication framework for wireless sensor networks, which is based on password and smart card and it uses one-way hash function. This scheme provides mutual authentication and gives user facility to change password at need. But the problem here is, it does not provide privileged insider attack as the password is sent to the base station in plain text. It also suffers from the synchronization problem as it uses the time stamp for avoiding replay attack.

Fan et al. [21] proposed an efficient and DoS-resistance user authentication scheme for two-tiered wireless sensor network. In this scheme user authenticates with Master Node / Cluster head in order to access information from the nodes in its cell. There is no provision to update the data table of user, so the user cannot be authenticated to Master Node not mentioned in data table even if he legitimate one if some urgent requirement arises. Another problem is synchronization. This scheme uses time stamp to avoid replay attack. But time synchronization in wireless sensor network is very difficult to achieve.

4. OVERVIEW OF ECC

Weierstrass equation for the elliptic curve is$y^2 = x^2 + ax + b$ in which a and b are real number. It is the simpler form of equation for the elliptic curve defined over the real number. The equation must satisfy $\Delta = -16(4a^3 + 27b^2) \neq 0$. Let$F_q$ denote the finite field of points, where q is a large prime number and containing x, y, a, b elements. $E$is a suitably chosen Elliptic curve defined over F_q. The points of the equation and the point at infinity O compose the elliptic curve group over real numbers. A large prime number $n$is selected such that $nP = O$ using the elliptic curve addition algorithm. Here nP means elliptic curve multiplication. $P$is a base point in the generator point E.Security of ECC relies on the difficulties of following problems [22].

Discrete Logarithm Problem (DLP): for a given pubic key point $F = \alpha P$, it is hard to compute the secrete key α.

Computational Diffie-Hellman Problem (CDHP): for given point elements αP and βP, it is hard to compute $\alpha\beta P$.

5. PROPOSED SCHEME

In this section, a user authentication scheme for WSNs is presented which assures the access and transfer of data to the legitimate user only. For that, first the user must register itself and on successful registration the base station personalizes a smart card to the registered user. Under network model mentioned in the Section 2, the entire WSN is divided into number of clusters. Each cluster is administered by cluster head. Each user has some device (like PDA) which has the ability to perform computational operations and commutate with cluster heads. Whenever user need some data it can authenticate itself to the network and access data collected within the cluster from the cluster head.

First the list of notations used in this proposed scheme is given. Finally, different phases related to this proposed scheme are described.

- $\boldsymbol{U_i}$: User i
- $\boldsymbol{ID_i}$: Identity of U_i
- $\boldsymbol{PW_i}$: Password of U_i
- $\boldsymbol{N_i}$: A secret random number known to U_i
- $\boldsymbol{BS}$: Base station
- $\boldsymbol{CH_j}$: Cluster head in j[th] cluster
- $\boldsymbol{ID_{CH_j}}$: Identifier of cluster head CH_j
- $\boldsymbol{S_n}$: Sensor node
- $\boldsymbol{x_a}$: A secret of base station
- $\boldsymbol{K}$: Symmetric key of BS
- $\boldsymbol{x_{CH_j}}$: A secret shared betweenCH_j and BS
- $\boldsymbol{h}(.)$: Cryptographic one-way hash function
- $\oplus$: XOR operator
- $||$: String concatenation operator
- $\boldsymbol{q}$: The order of the underlying finite field F_q
- $\boldsymbol{E}$: A suitably chosen Elliptic curve defined over F_q
- $\boldsymbol{P}$: A base point in the generator point E
- $\boldsymbol{n}$: The prime order of P
- $\boldsymbol{O}$:The point at infinity, where $np = O$ and $P \neq O$

In this scheme,SHA-1 is considered to be as secure hash function.$s_num$is number used to specify communication between cluster head and base station. It is automatically incremented with new session and last s_num for each cluster head is stored in database of base station.

5.1 Registration Phase

When a new user U_i wants to register himself/herself with WSN, he/she needs to perform following steps:

- The user U_i selects an identifierID_i, password PW_i and a random number N_i. Then U_i uses the random number N_i to compute masked password$MPW_i = h(PW_i||N_i)$. User U_i provides identifier ID_i and masked password MPW_i to the base station BS via a secure channel.
- If the above request is accepted, the base station BS computes $A_i = h(h(ID_i||x_a)||MPW_i)$, $B_i = h(ID_i||x_a) \oplus MPW_i$ and$C_i = h(x_a||K)$.
- Then BS issues a tamper-proof smart card withA_i, B_i,C_i and $h(.)$ stored in it.
- After receiving smart card user enters N_i into the smart card.

5.2 Login Phase

When user U_i wants to access real-time data from the WSN, he/she needs to perform following steps:

- User U_i inserts the smart card into the smart card reader then enters his/her identifierID_i and password PW_i into the reader terminal. Smart card computes the masked password of userU_i as $MPW_i^* = h(PW_i||N_i)$ and $a_i = B_i \oplus MPW_i^*$.
- Then it computes $A_i^* = h(a_i||MPW_i^*)$ and checks whether it is equal to the stored A_i. If not, then report wrong password PW_i to the user. This process performs up to some predefined number of times so that it can withstand password guessing attack by using stolen or lost smart card. If the above condition holds then smart card reader sends a $hello$ message to the BS.
- Upon receiving the $hello$ message the BS sends a random nonceRN_1 to the reader.
- Then the reader computes $DID_i = ID_i \oplus h(C_i||RN_1)$ and selects a random number $\alpha \in [2, n-2]$. After that it computes αP and$R_u = h(DID_i||\ \alpha P\ ||a_i\ ||RN_1)$.
- Sends a message$\langle DID_i, \alpha P, R_u, RN_1\rangle$ to the base station BS.

5.3 Authentication Phase

When BS receives login request message$\langle DID_i, \alpha P, R_u, RN_1\rangle$ from user U_i, it performs following steps to authenticate with the user U_i.

- BS first checks whether received RN_1 is fresh. If it is fresh then it computes$ID_i = DID_i \oplus h(h(x_a||K)||RN_1)$and $a_i^* = h(ID_i\ ||\ x_a)$ and uses $a_i^*$to compute$R_u^* = h(DID_i||\ \alpha P\ ||a_i^*\ ||RN_1)$.Then it checks if$R_u = R_u^*$. If it holds BS accepts the login request and proceeds to the next step.
- BS selects a cluster head nearest to the user. It retrieves s_num for that cluster head from its database. Then it computes $S_b = h\left(DID_i\ ||ID_{CH_j}\ ||x_{CH_j}\ ||\alpha P\ ||s\_num\right)$.
- BS sends a message$\langle DID_i, \alpha P, S_b, s_num\rangle$ to the corresponding cluster head CH_j.
- After receiving the message in previous step from BS, first CH_jchecks whether received s_num is greater than the saved s_num in its memory. If yes then it computes $S_b^* = h\left(DID_i\ ||ID_{CH_j}\ ||x_{CH_j}||\alpha P\ ||s\_num\right)$.Then cluster head checks if $S_b = S_b^*$. If it holds the cluster head accepts the login request and updates the previous s_num with the received s_num and proceeds to the next step.
- Then it selects a random number $\delta \in [2, n-2]$. After that it computes δP and$T_{CH_j} = h\left(DID_i||ID_{CH_j}\ ||x_{CH_j}\ ||\delta P\ ||s_num\right)$ and a session key $SK = \alpha\delta P$.
- The cluster head sends a message$\langle DID_i, ID_{CH_j}, \delta P, T_{CH_j}, s_num\rangle$ to the base station.
- After receiving the message in previous step from the cluster head, BS checks whether the received s_num is equal to the saved s_num for that cluster head in its memory. If it is equal then computes$T_{CH_j}^* = h\left(DID_i||ID_{CH_j}\ ||x_{CH_j}\ ||\delta P\ ||s_num\right)$ and checks if$T_{CH_j} = T_{CH_j}^*$. If it holds then it accepts the request. Then BS increments s_num by one and proceeds to the next step.
- Then it selects a random number $\gamma \in [2, n-2]$. After that it computes γP, $z = \alpha\gamma P$ and$V_\gamma = h\left(z\ ||\gamma P\ ||a_i\ ||ID_{CH_j}||\delta P\ ||RN_1\right)$.
- Then BS sends a message$\langle V_\gamma, \gamma P, ID_{CH_j}, \delta P, RN_1\rangle$ to the userU_i.
- After receiving the message in previous step from the BS, the userU_i checks whether receivedRN_1 is equal toRN_1in its temporary memory. If it is equal then user$U_i$computes $L = \alpha\gamma P$ and uses it to compute$V_\gamma^* = h\left(L\ ||\gamma P\ ||a_i\ ||ID_{CH_j}||\delta P\ ||RN_1\right)$. Then it checks if$V_\gamma = V_\gamma^*$. If it holds then user$U_i$ computes session key $SK = \alpha\delta P$.

The above generated session key is used in further communication between userU_i and cluster head CH_j.

5.4 Password Change Phase

Whenever userU_i wants to change his/her password, he/she has to perform following steps. Here all steps are performed locally. Involvement of the base station is not required.

- UserU_i inserts his/her smart card into the smart card reader. Then reader terminal asks the user to insert his/her identifierID_i, current passwordPW_i^{old}. After that smart card computes the masked value of current password as$MPW_i^{old} = h\left(PW_i^{old}\ ||N_i\right)$, $a_i = B_i \oplus MPW_i^{old}$ and$A_i^* = h\left(a_i||MPW_i^{old}\right)$.
- This computed A_i^* is compared with theA_i, which is stored in the smart card. If they do not match, then report wrong password PW_i to the user. This process performs up to some predefined number of times so that it can withstand password guessing attack by using stolen or lost smart card.
- Then it asks the user to enter new passwordPW_i^{new}.Then it computes the masked

value of new password $MPW_i^{new} = h(PW_i^{new} || N_i)$. Then it computes $A_i^{new} = h(a_i || MPW_i^{new})$ and $B_i^{new} = a_i \oplus MPW_i^{new}$.

- Finally, the stored A_i and B_i are replaced with A_i^{new} and B_i^{new} respectively in the smart card memory.

5.5 Dynamic Node Addition

In a wireless sensor network there are chances that some sensor nodes or cluster heads are captured by the attackers or they expire due to energy consumption. In that case new nodes are added to the network. In this proposed scheme as there is no common parameter shared between the users and cluster head as well as sensor node, so any number of nodes can be added to the network freely at any time. Here the same smart card is used to perform authentication with newly added cluster heads.

6. SECURITY ANALYSIS OF PROPOSED SCHEME

This section analyzes security of the proposed scheme which is based on security of ECC described in Section 3 and difficulties associated with one-way hash function.

This proposed scheme can resist against the following attacks.

User anonymity

In this proposed scheme, in each login request user anonymity is preserved. Suppose an attacker has intercepted a login request message $\langle DID_i, \alpha P, R_u, RN_1 \rangle$. But it cannot retrieve any static parameter from this message as all the values here are session dependent. Only base station can find ID_i from the DID_i as it has the knowledge of secret parameter x_a and its symmetric key K. Hence, in the presented scheme, an intruder or adversary cannot identify the user trying to login.

Privileged insider attack

In this scheme, the user does not send his/her password in plain text during registration. Here the password PW_i is first masked to produce MPW_i, which is $h(PW_i || N_i)$. It is computationally infeasible to find PW_i from MPW_i due to one way property of the hash function. So the privileged insider of the base station cannot know the password PW_i. Thus he/she cannot impersonate user in those servers where the user might have to register himself/herself with the same password. Thus this proposed scheme is resistance to the privileged insider attack.

Replay attack

In case of replay attack a legal entity's transmitted message is intercepted and that message is replayed later by an adversary. However in this scheme a random nonce is used to restrict replay message between user and base station and as s_num is used to restrict replay message between base station and cluster head.

Guessing attack

Consider the situation where user lost his/her smart card and it is found by an attacker or is stolen by an attacker. In that case attacker cannot impersonate that user by using the smart card because no one can find the password from the B_i without knowing the value of secrete x_a known only base station. This secret is also protected by cryptographic one-way hash function. The shared secrete a_i between U_i and BS is also protected in R_u and V_γ by same cryptographic one-way hash function. So this scheme is resistance to guessing attack.

Stolen verifier attack

As this scheme does not keep any password/verifier table at the base station or cluster head, so no one can steal password/verifier table. So it is resistance to stolen verifier attack. Here even in registration phase user does not send password directly to the BS. It is masked and sent to the base station to produce smart card. Then the masked password is deleted from temporary memory of base station.

Man-in-the-middle attack

Suppose an attacker intercept a login request message $\langle DID_i, \alpha P, R_u, RN_1 \rangle$, then it generates a random number α^* and computes $\alpha^* P$, which is later used to generate session key. But it cannot modify the login request message to $\langle DID_i, \alpha^* P, R_u^*, RN_1 \rangle$ as the attacker does not know the secret x_a, which is used to calculate R_u. Thus man-in-the-middle attack is not possible in this proposed scheme.

Mutual authentication

In case of mutual authentication both entities in a communication link authenticate to each other. In this proposed scheme mutual authentication is assured between cluster head (CH) and base station (BS). Here first BS is authenticated to CH_j using $S_b = h\left(DID_i || ID_{CH_j} || x_{CH_j} || \alpha P || s\_num\right)$. S_b can be computed only by CH_j and BS as the secret x_{CH_j} is known exclusively to CH_j and BS. Similarly CH_j is authenticated to BS using $T_{CH_j} = h\left(DID_i || ID_{CH_j} || x_{CH_j} || \delta P || s\_num\right)$.

The user is authenticated to BS by using $R_u = h(DID_i || \alpha P || a_i || RN_1)$ likewise BS is authenticated with the user using $V_\gamma = h\left(z || \gamma P || a_i || ID_{CH_j} || \delta P || RN_1\right)$. Only legitimate user which has the correct password can only extract a_i and hence can compute R_u. Similarly BS can compute V_γ as it has the secret x_a which is used to compute a_i.

Dos attack

Suppose an adversary has found or stole the smart card of a legitimate user U_i. However, in this proposed scheme, the smart card computes $A_i^* = h\big(h(ID_i || x_a) || h(PW_i || N_i)\big)$ and comparesit with the stored value of A_i in smart card's memory. This comparison will show the validity of user identity ID_i and password PW_i before the password update procedure. But the adversary cannot guess both user identity ID_i and password PW_i correctly in polynomial time. If login failure exceeds some predefined number of times, then the smart card will be locked immediately. Thus the proposed scheme is secure against denial of service attack.

Password change attack

This scheme is resistance to password change attack. Suppose for a stolen smart card if the attacker wants to change password he/she still must know the old password PW_i^{old}.

Smart card allows predefined number of times to enter correct the old password. If the attacker fails to enter the old password correctly then that smart card is blocked.

Many logged-in user with same login-id attack

This scheme can prevent the risk of many logged-in user with the same login ID as well as parallel session attack. Here login process starts only when the user inserts his/her card into the card reader and all computation is performed only during the period when the card is still inside the card reader. Once the card is removed the login process is terminated.

Smart card breach attack

Suppose a smart card is lost or stolen. Although it is assumed that a smart card cannot be cracked, an adversary may perform side channel attacks including differential power analysis and invasive attack and extract parameters like A_i, B_i,C_i andN_i. Then the adversary tries to impersonate the user to login to the Base Station. For that purpose adversary must be able to create a valid login request message$\langle DID_i, \alpha P, R_u, RN_1 \rangle$.
Here $R_u = h(DID_i || \alpha P || a_i || RN_1)$ and to compute a_i the adversary must have knowledge of either MPW_i orx_a. But adversary cannot find MPW_i as he does not have knowledge of PW_i and he also cannot extractx_a from theC_i as it is protected by one-way hash function. Thus the proposed scheme can resist smart card breach attack.

Resilience against node capture attack

As sensor nodes and cluster heads are deployed in a hostile environment, they can easily capture by an adversary. So the adversary can steal the stored secret information in those nodes. Suppose some cluster heads are captured by an attacker. So the attacker knows the secret x_{CH_j} stored in the cluster head. As x_{CH_j} for each cluster head is different and they are stored in the cluster heads before deployment, so only those cluster heads will send false data to the user. But other non-compromised node will continue to communicate securely with the users. That means compromise of some captured cluster heads does not affect secure communication between other non-compromised cluster heads and users. So this scheme is resilience against node capture attack.

Masquerade Attack

Suppose an adversary wants to impersonate himself as a legal user to the WSN. Then he must compute a validDID_i andR_u which will be sent to base station with login request. But$DID_i = ID_i \oplus h(C_i || RN_1)$
and $R_u = h(DID_i || \alpha P || a_i || RN_1)$ where $C_i = h(x_a || K)$ and$a_i = h(ID_i || x_a)$. Only the base station has the knowledge of secretx_a and symmetric key K. So adversary cannot create a validDID_i andR_u as he does not know the value ofx_a and K. So this scheme is resistance to masquerade attack.

Table 1.Comparison of enhanced security features of the proposed scheme with other schemes

Security Feature	Proposed Scheme	Watro et al.	Wong et al.	ML Das	Khan and Alghathbar	Kumar et al.	Fan et al.
S_1	Yes	Yes	No	No	Yes	No	No
S_2	Yes	No	No	No	Yes	Yes	No
S_3	Yes	Yes	No	No	Partial	Partial	Yes
S_4	Yes	No	No	No	No	No	No
S_5	Yes	No	No	No	No	No	Yes
S_6	Yes	No	No	No	No	No	No
S_7	Yes	Yes	No	No	No	No	No

S_1: Privileged Insider Attack S_2: Support Password ChangeS_3: Mutual AuthenticationS_4: Resilient Against Node CaptureS_5: Provide Secret Session KeyS_6: Support Dynamic Node AdditionS_7: Resistance to Time Synchronization

Table 2.Comparison of computational cost in different phases of proposed scheme with other schemes

Phase	Entity	Proposed Scheme	Watro et al.	Wong et al.	Das	Khan and Alghathbar	Kumar et al.	Fan et al.
Registration	User	t_h	$t_{pu} + t_{pr}$	-	-	t_h	-	-
	BS	$3t_h$	-	$3t_h$	$3t_h$	$2t_h$	$3t_h$	$6t_h$
	Sensor	-	-	-	-	-	-	-
	CH	-	-	-	-	-	-	-
Login + Authentication	User	$5t_h + 3t_{em}$	$2t_{pr} + t_h$	-	$4t_h$	$4t_h$	$4t_h$	t_h
	BS	$7t_h + 2t_{em}$	-	t_h	$4t_h$	$5t_h$	$5t_h$	$2t_h$
	Sensor	-	$2t_{pu} + t_h$	$3t_h$	t_h	$2t_h$	$2t_h$	$2t_h$
	CH	$2t_h + 2t_{em}$	-	-	-	-	-	$8t_h$

t_h: hash computation t_{em}:elliptic curve point multiplication t_{pu}:public-key computation t_{pr}:private-key computation

7. COMPARISON WITH RELATED SCHEMES

In this section the performance of the proposed scheme is compared with some selected existing related schemes: Watro et al. [7] scheme, Wong et al. [10] scheme, ML Das [15] scheme, Khan and Alghathbar [16] scheme, Kumar et al. [20] scheme and Fan et al. [21] scheme.

In Table1, the comparison of security feature among different schemes is presented. Here it shows that the proposed scheme is stronger in terms of security. Our scheme along with Watro et al. [7] and Khan and Alghathbar [16] provides protection against privileged-insider attack. Password change or update feature is supported by our scheme, , Khan and Alghathbar [16] and Kumar et al. [20] scheme Whereas only our scheme is resilient against node capture attack. Mutual authentication is supported by our scheme, Watro et al. [7] and Fan et al. [21] scheme. Only our scheme and Fan et al. [21] scheme establishes secret session key between the user and sensor/cluster head. Only our scheme provides an option for dynamic node addition. In our scheme time synchronization is not needed to provide protection against replay attack.

In table 2,thecomparison of computational cost in different phases of the proposed scheme with other schemes is given. Here the computation cost for XOR is not considered as it is negligible. This scheme uses cluster head to authenticate with user and cluster head is more resource-rich compared to usual sensor node. This scheme uses the advantage of using computational power of base station and cluster head to provide more secure login to user.

Lastly, considering computation cost at sensor node/cluster head, the proposed scheme uses two hash operation and two elliptic curve multiplication in whole authentication process. As cluster heads have more computing power and energy resources so above operations are feasible. The proposed scheme is also stronger than other scheme in term of security. It includes six message transfers in whole authentication process. The first two messages are to receive random nonce from the base station. This random nonce helps this scheme from time synchronization problem which is a very difficult task in case of WSN. Considering over all scenarios this scheme is better than all other schemes.

8. CONCLUSION

In this paper, a user authentication scheme based on elliptic curve cryptography for large scale hierarchical wireless sensor networks is presented. Here, feasibility of ECC in context of WSN is demonstrated. It provides mutual authentication between user and base station as well as base station and cluster head. The proposed scheme also provides option for dynamic node addition where there is no need to update any information in user smart card for accessing real time data for any addition or replacement of cluster heads in the networks. It provides a secret session key for further communication between user and the cluster head. This scheme implements merit of using ECC-based mechanism in WSN and enhances the WSN authentication with higher security than other protocols.

9. REFERENCES

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. “Wireless sensor networks: a survey”. Computer Networks 2002, 38(4):393–422.

[2] Kalra, S. and Sood, S. K. “Elliptic curve cryptography: survey and its security applications”. In Proceedings of the International Conference on Advances in Computing and Artificial Intelligence (ACAI '11). ACM, New York, NY, USA, 102-106. 2011

[3] Wang, H., Sheng, B., Tan, C. C. and Li., Q. “Public-key based access control in sensornet”. Wirel. Netw. 17, 5 (July 2011).

[4] Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S. C. “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks”. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications (PERCOM '05). IEEE Computer Society, Washington, DC, USA, 324-328. DOI=10.1109/PERCOM.2005.18.

[5] Rivest, R. L., Shamir, A. and Adleman, L. M. “A method for obtaining digital signatures and public-key cryptosystems”. Communications of the ACM 1978; 21:120–6.

[6] Diffie, W., Hellman, M. E. “New directions in cryptography”. IEEE Transactions on Information Theory 1976; 22:644–54.

[7] Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., Kruus, P. "TinyPK: securing sensor networks with public key technology". In: Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks, SASN 2004, Washington, DC, USA; October 2004. p. 59–64

[8] Benenson, Z., Gartner, F. and Kesdogan, D. "User Authentication in Sensor Networks" (Extended Abstract), Lecture Notes in Informatics Proceedings of Informatics 2004, Workshop on Sensor Networks, Ulm, Germany, September 2004.

[9] Benenson, Z., Gedicke, N. and Raivio, O. "Realizing Robust User Authentication in Sensor Networks", in the Workshop on Real-World Wireless Sensor Networks, Sweden, June 2005

[10] Wong, K., Zheng, Y., Cao, J., Wang, S. "A dynamic user authentication scheme for wireless sensor networks". In: Proceedings of IEEE international conference on sensor networks, ubiquitous, and trustworthy computing, IEEE Computer Society; 2006. p. 244–51.

[11] Banerjee, S. and Mukhopadhyay, D. "Symmetric Key Based Authentication Querying in Wireless Sensor Networks", in Proceedings of the First International Conference on Integrated Internet Ad Hoc and Sensor Networks, Nice, France, May 30-31, 2006.

[12] Blundo, C., Santis, A. D., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M. "Perfectly-secure key distribution for dynamic conferences", in Advances in Cryptology CRYPTO 92, LNCS 740, pp. 471486, 1993.

[13] Jiang, C., Li B. and Xu H. "An Efficient Scheme for User Authentication in Wireless Sensor Networks" 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) 2007.

[14] Tseng, H. R., Jan, R. H. and Yang, W. "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks", GLOBECOM 2007

[15] Das, M. L. "Two-factor user authentication in wireless sensor networks". IEEE Transactions on Wireless Communications 2009; 8(3):1086–90.

[16] Khan, M. K., Alghathbar, K. "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks". Sensors 2010; 10:2450–9.

[17] He, D., Gao, Y., Chan, S., Chen, C. and Bu, J. "An enhanced two-factor user authentication scheme in wireless sensor networks". Ad Hoc & Sensor Wireless Networks 2010;10(4).

[18] Omar Cheikhrouhou, AnisKoubâa, ManelBoujelben and Mohamed Abid , "A Lightweight User Authentication Scheme for Wireless Sensor Networks", The ACS/IEEE Workshop : Future Trends on Ad-hoc and Sensor Networks (FTASN2010), Hammamet, Tunisia, May 16-19, 2010.

[19] Tseng H. R., Jan R. H. and Yang W. "A robust user authentication scheme with self-certificates for wireless sensor networks" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks (2010) Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/sec.212

[20] Kumar, P., Sain, M. and Lee H. J. "An Efficient Two-Factor User Authentication Framework for Wireless Senor Networks" ICACT 2011

[21] FAN, R., HE D. J. and PAN, X. Z. Ling-di PING "An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks" Journal of Zhejiang University-SCIENCE C (Computers & Electronics) ISSN 1869-1951 (Print); ISSN 1869-196X (Online) Received Oct. 27, 2010; Revision accepted Feb. 23, 2011; Crosschecked May 30, 2011

[22] Li, F., Xin, X. and Hu, Y. "Identity-based broadcast signcryption". Computer Standard and Interfaces 2008;30:89–9

[23] Cheng, Y. and Agrawal, D. P. "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks." Ad Hoc Networks 2007;5(1):35–48