Light Weight Authentication framework for WSN

Ayaz Hassan Moon
National Institute of Electronics and Information Technology ,Srinagar, J & K.

Ummer Iqbal
National Institute of Electronics and Information Technology ,Srinagar, J & K.

G. Mohiuddin Bhat
Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, J & K.

***Abstract*— Primarily deployed for monitoring environmental parameters,WSN are now finding increased use in commercial, domestic, military and health applications. There deployment in hostile terrains and for mission critical applications touching human lives call for addressing their security issue. Especially under IoT and smart city projects like Padova Smart City project, the range of applications envisioned to be developed, would be tightly coupled to the physical world where security aspects would be paramount.**

This paper presents a light weight Authentication Framework which supports node registration, entity authentication, key establishment, new node injection and broadcast authentication of messages diffusing from base towards nodes in WSN. The solution leverages the low computational overheads associated with cryptographically secure one-way hash chains and ECC without using any digital signature algorithm. The usage of hidden generator point derived by using hash-chains provides defence against man-in-the middle attack a prominent feature in ECDH. The proposed framework is compared with other similar Schemes like Novel Access Control Protocol for secure Sensor Networks (NACP).

Keywords— Access Control List; Entity Authentication; Hidden Generator;Wireless Sensors Network

I. INTRODUCTION

Wireless Sensor Networks presents enormous scope for building wide range of applications due to its low cost , tiny size and ease of deployment [1]. However, there are several security challenges to be surmounted to fully realize the advantages due to ubiquitous nature of WSN. Communication being broadcast in nature is more prone to different kind of attacks like eves dropping, intercept, inject and alter transmitted data [2]. In conventional networks, authentication, data integrity and confidentiality is achieved through end-to-end mechanism like SSH, SSL, IP-Sec. In end-to-end communication it is neither necessary nor desirable for the contents of the message, beyond headers, to be made available to intermediate routers [3]. The case is different for WSN. The dominant traffic pattern is many-to-one implemented over multi-hop topology in which in-network processing and data aggregation has to be undertaken by intermediate nodes. This is possible only if the nodes can access sensor data. Therefore link layer security is an appropriate solution for such networks rather than embarking on end to end security solutions [4].

WSN networks are characterized by severe resource constraints in terms of energy, computational power, bandwidth and storage. The typical characteristics of a MicaZ mote are 8-Bit micro-controller,ATmega128L with 4 KB of RAM, 128 KB of ROM, bandwidth of 250kbps and is powered by two AA lithium cells with 2000mAH of energy [5].The operating system along with the storage required for sensed data occupies almost half of its memory resource, leaving the rest for the application code. Similarly, the energy reserves are estimated to last for 4 days of continuous operation, assuming 18 ma and 3 micro amperes of current drain during active and sleep mode respectively of a mote powered by 2AA cells.

Traditional cryptographic algorithms employing Public crypto are highly resource intensive to directly fit into the WSN architecture [6][7]. Therefore ECC has emerged as a computationally efficient scheme for resource constraint sensor hardware platform especially in the context of IOT and Smart City applications [8][9][10]. Among all the security primitives, authentication which may also cover data integrity, data freshness and sequencing is the most important requirement. Barring certain cases involving military and reconnaissance, confidentiality may not be the requirement as the authentication would be [11][12].

A. Authentication Requirement:

Authentication encompasses important security services to ascertain that data has originated from the alleged source and has not been modified en route. Its implementation enforces the mitigation of active attacks like Denial of service and impersonation. Authentication covers both the aspects related to network entity and message. The entity authentication is realized when both the claimant and the verifier exchange communication in real time without revealing any meaningful information other than the claim of being a particular entity. While as message authentication in itself does not provide any timeliness guarantee in terms of as to when the message was created. The resource constraint nature of WSN almost pre-empties the use of conventional Public Key Cryptography schemes and digital signatures based on RSA. Even ECC based digital signature scheme ECDSA is computationally intensive and its frequent use can lead to energy exhaustion.

In WSN , deployment of nodes is not generally done in any ordered or engineered fashion. Some of the Nodes could therefore be compromised which need to be detected and

revoked from the network. Also, Energy exhaustion of the deployed nodes may lead to their death thereby reducing the number of active nodes within the network. This implies that addition of new nodes into the network becomes inevitable to sustain and prolong the life of the network. This makes WSN vulnerable to the addition of malicious nodes by an adversary[13] .To mitigate this problem, a proper access control mechanism has to be enforced within the network which could broadly have two levels:

- Entity Authentication
- Proper Key Establishment.

B. *Entity authentication*

Authentication is an assurance about the identities of communicating nodes or principals in any network. It involves a process to ascertain that the data has come from the alleged source and has not been modified en route. Authentication works at two levels: one at the level of entity called as entity authentication or Identity and other at the level of data called as message authentication also known as data integrity. [12],[13].

C. *Key establishment*

Key establishment plays a pivotal role in ensuring authentication. An uncomplicated yet efficient method to share secret keys in WSN is based on ECDH.. However ECDH suffers from Man-in-the-Middle Attack. The Man-in-the-Middle-Attack can be overcome by using Hidden Generator Point concept and proper authentication mechanism [14].

II. CONTRIBUTION OF THIS PAPER

This paper presents a light weight entity authentication framework to support an access control mechanism in WSN. The proposed work facilitates node registration, entity authentication, key establishment, new node injection and Broadcast authentication of messages diffusing from base towards nodes. The solution leverages the low computational overheads associated with cryptographically secure one-way hash chains and ECC [15][16] without using any digital signature algorithm associated with authenticated broadcasts. The usage of hidden generator point derived from hash-chains provides defence against man-in-the middle attack.

Rest of the paper is organised as following: Section III provides an insight about the related work, Section IV describes the detailed Authentication Framework design in 6 phases, Section V highlights the security analysis of the proposed scheme, while as Section VI concludes the paper.

III. RELATED WORK

Hash Chains were first proposed by Lamport who used it for generating one-time password [17]. This involves applying a hash function h(.) repeatedly z times to a seed s to form a hash chain of length z. The hash (.) is easy to compute but hard to invert.e.g, h(h(h(s))) gives a hash chain of length 3 and can be denoted by $h^3(s)$.The initial element of the hash chain is called the seed and the last element is called committed value or the tip of the hash chain. The tip of the chain is public and is distributed among the nodes and the elements of the chain are consumed one after other until secret key is free. Hash chains find exclusive use in data integrity and entity authentication. The ith element of the hash chain denoted as K_i is expressed as:

$K_i(s)= h(h^{z-i}(s))$ The committed value of the chain is made public while as the seed acts as private or secret value.

The scheme does not overcome the need for an authenticated initial key-exchange. By the definition of entity authentication, Lamport's one-time passwords do not provide entity authentication as there is no proof of an active communication between the two parties.

An access control protocol based on ECC and ECDSA was initially put forth by Zhou et al [18]. It proved to be more efficient than conventional PKI scheme based on RSA. The scheme is based on node identity and node boot strapping time to achieve authentication. It can add fresh nodes, support key establishment and use timestamps to protect against replay attack. The protocol had implementation issues related to its assumption of tolerance time interval for sustaining an attack and bootstrapping time. Huang proposed a novel access control protocol for secure sensor networks(NACP) which is primarily based upon Zhou et al scheme [19]. The scheme makes use of Hash chains and Elliptical curve cryptography. Besides its simplicity, the protocol offers efficient authentication mechanism at low energy costs, which makes it suitable for WSN. NACP does not us use any timestamp and is not based on the assumption of tolerance time interval to sustain the attack.

Another scheme , A new Dynamic Access Control Protocol (NDACP) by H.Huang et al, utilizes cryptographically light, hash functions and XOR operations to achieve node to node mutual authentication [20] .

Initially, Security architectures like SPINS [21] , LEAP [22] and TinySec [23] have been built based on different assumptions. Perrig et al (2002) introduced "Security Protocols for sensor Networks " (SPINS). SPINS comprises of sensor network encryption protocol (SNEP) and µTESLA. SNEP provides confidentiality, two party data authentication, integrity and freshness. Through a process of randomization of Initialization vectors and use of counters, SNEP achieves semantic security, which means the same plain text is encrypted differently each time the counter value is incremented. All cryptographic primitives i.e, encryption, message authentication code (MAC), hash, random number generator are constructed out of a single block cipher for code reuse. TinySec was designed by Karlof, Wagner, Shastri (2004) inherently to provide similar services as provided by SPINS. A major difference between TinySec and SNEP is that there are no counters used in TinySec besides TinySec uses MAC length of 4 bytes and SPINS using 8 bytes. However TinySec needs re-keying.

TESLA is a broadcast authentication protocol. It authenticates the initial packet with a digital signature, which

is expensive for sensor nodes. µTESLA proposed by Perrig et al (2002) provides authenticated data broadcasts for severely resource-constrained environment like that of WSN. To authenticate the broadcast messages, µTESLA uses delayed key disclosure and one-way hash function to generate key chain . The base station selects a random value Kn as the last key in the key chain and repeatedly performs a pseudorandom function F to compute all the other keys:

$$K_i = F(K_{i+1}) \quad ; \quad 0 \le i \le n-1 \qquad (1)$$

Where the secret key K_i (except K_0) is assigned to the ith time interval. With the help of the initial key K_0, which is called the chain commitment, receiver can authenticate any key in the chain by performing pseudorandom hash function operations. The scheme is subject to DOS attack which can lead to buffer overflow and battery exhaustion.

Certificate-based public key authentication system has been used widely in the wired network, such as the PKI(Public Key Infrastructure) system, in which for authentication both the sides must hold a certificate issued by the third party called CA(Certification Authority) . The two sensor nodes need to have the same configuration at the same time. The authentication scheme of TinyPK-RSA [24] can be used conveniently to realize the WSN entity authentication based on this scheme. The constraints of WSN present serious inhibition to such method.ECC have shown more promise for application of asymmetric techniques for authentication in WSN. ECC can achieve same level of security as RSA with a smaller key size e.g. 160 Bit ECC can provide comparable security to the conventional 1024 Bit RSA. Smaller key size often brings the advantage of faster computation efficiency and saving of bandwidth, memory and energy. Therefore ECC is better suited for resource constrained devices like WSN.

IV. AUTHENTICATION FRAMEWORK DESIGN

The proposed authentication framework has been designed to present a comprehensive pair-wise entity authentication protocol with proper key establishment . The proposed framework has been compared to different Access Control schemes in WSN like the one proposed by Y. Zhou et al and NACP by Huang [25] and addresses the issues found in these schemes listed as under:

- Zhou et al scheme is based on ECC and ECC based digital signature scheme ECDSA. It is energy efficient than RSA. It achieves node authentication and key establishment for new nodes by including both node identity and node bootstrapping time into the authentication procedure. However it uses timestamps and assumes that each sensor node can sustain time interval before it can be compromised. Therefore for practical implementations it is not thought to be convenient.
- NACP [19] scheme proposed by Huang is based on Hash chains and ECC. It is simple, energy efficient, supports new node addition but has been found to be vulnerable to replay attack and new node masquerading attacks. This is attributed to absence of any mutual authentication between node and base station. It also lacks hash chain renewability.
- There is no node registration phase in both the schemes where in the nodes after deployment could register themselves with the base station before they are bootstrapped to launch authentication.
- The above schemes lack authentication mechanism for conveying updated hash chain values.

The Proposed scheme addresses the above issues and spans the framework over the following 6 phases:
Initialization phase, Node registration phase, Node Authentication and Key generation phase, Node to Node Authentication, Base Station Broadcast for new hash chain , New node injection phase

TABLE 1. NOTATIONS USED

Symbol	Notation
h()	One way-hash function
p	A prime number
Zp	A finite field
Ep	Elliptic curve
G,Ga,Gb	Generator point of order n
Ni	Node identity of ith node
Nj	Node identity of jth node
BS	Base station
Ki	Secret key of ith node
Kj	Secret key of jth node
Ks	Secret key of base station
z	Large integer
hm(k)	m cascade hash operations on key k
xij	Sessions key establishment between ith node and jth node
$\oplus$	XOR Operation
||	Concatenation Operator

A. Initialization phase

Let there be r nodes with N_1, N_2,---,N_r as their identities constituting the neighborhood of a WSN. The node identities are integer numbers. Base station (BS) selects secret key ks and computes its hash chain $h^z(k_s)$ by applying the select hash function h(.) z times over ks. BS also generates r number of secret keys k_1, k_2,----k_r for each of the node. It calculates $h_z(k_i)$ as hash-chain commitment of each node with i= 1, 2, 3,----,r by repeatedly applying hash function z times. Further BS initiates following actions:

- It preloads each of the Node Ni with its associated secret key K_i (seed) and one-way hash function h().
- It calculates its own hash chain commitment $h^z(ks)$ and preloads it in all the nodes.
- It selects an elliptic curve Eq, a cyclic group G and preloads its associate parameters like G, n,a,b,p,H in all the nodes.

B. Node Registration phase

In the post deployment phase, each node has to register itself with the base station before it can communicate with the other nodes in its neighborhood.

Step 1: $N_i \longrightarrow Base : h(N_i \oplus ki), N_i \qquad (2)$

The purpose of this step is to register in the access control list of BS the legitimate nodes which have valid pre deployed keys as assigned to them by BS.
N_i hashes the XOR of its node-id N_i with its secret key K_i and sends it to base along with its node-id.

Step 2: BS Verifies the $h(N_i \oplus k_i)$ by using the k_i from its own storage and N_i from the Step 1. If the verification holds, then base station adds node N_i to its access control list and broadcasts the hash chain $h^z(k_i)$ to the network. The authenticated broadcast of base station to the nodes is achieved in the following steps:

$$BS \longrightarrow *: \; h(h^{z-1}(k_s) \,||\, (h^z(k_i) \oplus N_i) \,||\, nB) = z_i \qquad (3)$$

$$BS \longrightarrow *: \; (h^z(k_i) \oplus N_i), h^{z-1}(k_s), N_i, nB \qquad (4)$$

$h^{z-1}(k_s)$, the secret chain value of BS which can be computed by BS only and has the significance of private key to BS . nB is a nonce and has been added to mitigate replay attack.

Step 3. On receiving the above broadcast, nodes in the network including N_i first verify the expression:

$$h(h^{z-1}(k_s)? = h^z(k_s). \qquad (5)$$

If found true, (which implies that it has originated from BS) then the expression:

$h(h^{z-1}(k_s) \,||\, (h^z(k_i) \oplus N_i) \,||\, nB)$ is evaluated and compared with the BS broadcast z_i . If it holds, then the hash chain commitment $h^z(k_i)$ of N_i is extracted from $(h^z(k_i) \oplus N_i)$ and registered in their access control list along with the node id, N_i. The hash chain of BS is updated to $h^{z-1}(k_s)$.

C. Node authentication and key generation

For the purpose of pair-wise symmetric key generation, the scheme uses Hidden Generator Concept of ECC along with the hash chains. Suppose a pair of nodes i.e. N_i and N_j , which are in each other's radio range want to communicate with each other. Let z be the hash chain length of both the nodes. Let N_i and N_j have successfully completed u and v times authentications respectively.

Key generation step using hidden generator:

We follow the essence of Hidden Generator Concept which assumes that the two nodes have different Generator points Ga and Gb for the elliptic curve Eq , which have not been made public. This technique of not publicly disclosing the generator point would help in mitigating the man-in-the-middle attack.

Ist Exchange between N_i and N_j

$$N_i \longrightarrow N_j : Ga.(h^{z-1}(k_i)).N_j \qquad (6)$$

$$N_j \longrightarrow N_i : Gb.(h^{z-1}(k_j)).N_i \qquad (7)$$

The scalar multiplication of hash chain secret and node identities with the respective generator points shall result in a point on the elliptic curve. It will also associate node identity with the process of key generation.

2nd Exchange between N_i and N_j

Nodes will exchange their hash chain secrets.

$$N_i \longrightarrow N_j : h^{z-1}(k_i) \qquad (8)$$

$$N_j \longrightarrow N_i : h^{z-1}(k_j) \qquad (9)$$

Verification Phase

N_i verifies $h(h^{z-1}(k_j)) ?= h^z(k_j)$, if true, then it computes :

$$Gb.[h^{z-1}(k_j)].N_j.[h^{z-1}(k_j)]^{-1}.[N_j]^{-1} = Gb \qquad (10)$$

N_j verifies $h(h^{z-1}(k_i)) ?= h^z(k_i)$, if true, then it computes :

$$Ga.[h^{z-1}(k_i)].N_i.[h^{z-1}(k_i)]^{-1}.[N_j]^{-1} = Ga \qquad (11)$$

Shared key between N_i and N_j:

Now after 4 exchanges as indicated from (6) to (9), N_i has the knowledge of Gb that is the generator point of N_j and N_j has the knowledge of Ga that is the Generator point of N_i.
N_i and N_j arrive at a Common Generator Gs = Ga+Gb.
Gs is a point on the elliptic curve $P(x_s,y_s)$.
The shared key between N_i and N_j shall be the x co-ordinate of point P i.e, x_s .The pairwise key established between N_i and N_j i.e., $K_{ij} = x_{ij}$

D. Node-Node Authentication:

Node to Node Authentication is based upon verification of hash chain commitment of each node, node identity and the shared key between them. If either of the verification tests fails, then the authentication will not be completed. Assuming Let N_i and N_j have successfully completed u and v times authentications respectively.
N_i computes the following and sends it to N_j:

$$N_i \longrightarrow N_j : h(h^{z-u-1}(k_i) \,||\, N_j) = a_i \qquad (12)$$

$$N_i \longrightarrow Nj : h(h^{z-u-1}(k_i) \,||\, x_{ij}) = a_k \qquad (13)$$

N_i broadcasts $h^{z-u-1}(k_i)$ and N_j.
Similarly N_j computes the following and sends it to N_i:

$$N_j \longrightarrow N_i : h(h^{z-v-1}(k_j) \,||\, N_i) = b_j \qquad (14)$$

$$N_j \longrightarrow N_i : h(h^{z-v-1}(k_j) \,||\, x_{ij}), = b_k \qquad (15)$$

N_j broadcasts $h^{z-v-1}(k_j)$ and N_i

Verification phase:
N_i performs the following calculations:

$$h(h^{z-v-1}(k_j))? = h^{z-v}(k_j) \quad (16)$$

If found correct then N_i verifies the following expression:

$$h(h^{z-v-1}(k_j) \,||\, N_i)?= bj \quad (17)$$

$$h(h^{z-v-1}(kj)|| \, xij) = bk \quad (18)$$

N_i authenticates N_j
N_j evaluates the following expressions:

$$h(h^{z-u-1}(k_i))? = h^{z-u}(k_i) \quad (19)$$

If found correct then N_j verifies the following expression:

$$h(h^{z-u-1}(k_i) \,||\, N_j) \,?= a_i \quad (20)$$

$$h(h^{z-u-1}(k_i)|| \, x_{ij}) \;?= a_k \quad (21)$$

If both the verifications hold, then Nj authenticates Ni.

Upon successful authentication , N_i upgrades its hash chain to $h^{z-u-1}(k_i)$ and N_j upgrades its hash chain to $h^{z-v-1}(k_j)$. It conveys the same to the BS.

E. Base Station broadcast for New Hash Chain Commitment:

Base Station Broadcasts the updated hash-chain commitment for N_i and N_j as $h^{z-u-1}(k_i)$ and $h^{z-v-1}(k_j)$ respectively in an authenticated manner by using its secret hash chain value i.e. $h^{z-s-1}(k_s)$ in the following manner :

$$BS \longrightarrow * : h(h^{z-s-1}(k_s)) \,||\, (h^{z-u-1}(k_i) \oplus N_i) \quad (22)$$

$$BS \longrightarrow * : h(h^{z-s-1}(k_s)) \,||\, (h^{z-v-1}(k_j) \oplus N_j) \quad (23)$$

BS broadcasts : $(h^{z-u-1}(k_i) \oplus N_i)$, $h^{z-s-1}(k_s)$, N_i and $(h^{z-v-1}(k_j) \oplus N_j)$, $h^{z-s-1}(k_s)$, N_j.

Verification:

Nodes first verify if $h(h^{z-s-1}(k_s)) \,?= h^{z-s(}k_s)$.

If it holds, then each node extracts $h^{z-u-1}(k_i)$ and $h^{z-v-1}(k_j)$ from the (22) and (23) as the new hash value of N_i and N_j. With every broadcast the hash-chain of BS is also updated to new value as $h^{z-s-1}(k_s)$.

F. New node injection phase:

Let a new node N_{r+1} is to be added to the network. The following steps will have to be initiated:

Step 1 Base station (BS) generates a random number k_{r+1} as the secret key of new node N_{r+1}. It preloads the Node N_{r+1} with its associated secret key K_{r+1} (seed) ,one-way hash function h() and current hash chain commitment of base station $h^{z-w}(ks)$.

- It calculates the hash chain commitment of new node N_{r+1} as $h^z(k_{r+1})$.
- It selects an elliptic curve Eq and preloads its associate parameters like G, n,a,b,p,h in $N_{r+1.}$

Step 2 On deployment, N_{r+1} registers itself with the base station by initiating following steps:

$$N_{r+1} \longrightarrow Base : h\,(N_{r+1} \oplus k_{r+1}),\, N_{r+1} \quad (24)$$

BS Verifies the $h\,(N_{r+1} \oplus k_{r+1})$, by using the k_{r+1} from its own storage and N_{r+1} from the above expression. If the verification holds, then base station adds node N_{r+1} to its access control list and broadcasts the hash chain $h^z(k_{r+1})$ to the network. Assuming the current hash chain value of BS is $h^{z-w}(k_s)$ then the authenticated broadcast of base station to the nodes is achieved as indicated under

$$BS \longrightarrow * :h(\, h^{z-w-1}(k_s) \,||\, (h^z(k_{r+1}) \oplus N_{r+1}) \,||\, nC) = z_i \quad (25)$$

$$BS \longrightarrow * : \; (h^z(k_{r+1}) \oplus N_{r+1}),\, h^{z-w}(k_s), N_{r+1}, nC \quad (26)$$

Step 3. Nodes in the network including N_{r+1} first verify the expression:

$$h(\, h^{z-w-1}(\,(k_s))? = h^{z-w}(k_s). \quad (27)$$

If found true (which implies that it has originated from BS) then the expression:

$$h(h^{z-w-1}(k_s) \,||\, (h^z(k_{r+1}) \oplus N_{r+1}) \,||\, nC) \quad (28)$$

is evaluated and compared with the BS broadcast z_i . If it holds, then the hash chain commitment $(h^z(k_{r+1}))$ of N_{r+1} is extracted from :

$$(h^z(k_{r+1}) \oplus N_{r+1}) \quad (29)$$

and registered in their access control list with the node id as $N_{r+1.}$

V. Security Analysis:

A. Man-in-the-middle attack:

Man-in-the-middle attack is normally launched due to lack of authentication between the communicating entities as is prominent in ECDH. An adversary can also launch MIM by misusing the public disclosure of Elliptical Curve Parameters especially the Generator Point.
In our proposed scheme, the concept of hidden generator has been used, wherein communicating nodes make exchanges to arrive at a common generator point which is not known to the other entities. Moreover Shared key generation has been tied to Node identities which make the scheme more robust against MIM attack.

B. Instant authentication:

In a Broadcast authentication protocol like μ-tesla , nodes cannot authenticate the packets instantaneously because of the delayed disclosure of keys. This can be exploited by an adversary who can inject forged messages into the network and launch denial of service attack .In our proposed scheme instant authentication is provided upfront, by verifying the hash chain secret value before evaluating other expressions .Packets need not to be buffered for authentication as done in case of μ-tesla.

C. Malicious node Injection:

A node is to first register itself with the base station during Registration phase by making use of Node id and secret key k_i. It is only on successful registration, the hash chain commitment is communicated to the node by the base station. This step prevents a malicious node to join the network as it cannot participate in the network communication without forcing its entry into the Access control list of BS.

D. Authenticated broadcast:

In our proposed scheme, all the broadcast emanating from base station like; Initial Hash commitment of the nodes and updated Hash Commitments of the nodes, are made by making use of the secret hash values of base to get it authenticated by the nodes. For example no one has the ability to generate the secret hash value $h^{z-w}(k_s)$, after w number of successful authenticated broadcast , except for the BS. Similarly nodes use hidden generator point and secret keys to convey their updated hash chain values to the BS which serves as an entity authentication of nodes.

VI. Results and Comparison

The computational cost of the proposed scheme is as following:

*Authentication Cost:((4*TEM)+ (6*TH))*
*Hidden Generator Point((4Key Exchanges) + (4*TEM) + (2 Inverse Operations))*

Where *TEM* is Point Multiplication over an elliptic curve and *TH* is Time for executing one-way hash function

Table 2 gives comparison of our proposed scheme in terms of Point Multiplication over an elliptic curve (TEM) and Time for executing one-way hash function (TH) with some of the other protocols as illustrated in the survey of access control schemes in WSN given by Youssou Faye et al [25]. In terms of total cost our scheme is comparable to NACP, PACP and ENACP with the additional advantage of offering authenticated broadcast by BS. It also builds inherently protection against MIM attack by using Hidden generator concept [26].
The Hidden generator scheme used for generation and establishment of pair wise keys has been compared with ECDH and the one given by Ravi et al [27].Our scheme has low computational cost and less number of broadcasts as compared to Ravi et al as shown in Table 3.

TABLE 2:COMPARISON OF OPERATION FOR DIFFERENT AUTHENTICATION SCHEMES

Scheme	Computations for achieving authentication for each node		
	TEM	***TH***	***Total cost***
Yun Zhou et al	3	1	4
NACP	2	5	7
ENACP	2	8	10
PACP	2	5	7
NDACP	5	-	5
Our scheme	4	6	10

TEM: Point Multiplication over an elliptic curve

TH: Time for executing one-way hash function

TABLE 3: COMPARISON OF OPERATION FOR ESTABLISHING HIDDEN GENERATOR POINT.

Scheme	Total Number of Exchanges to establish key	Total number of Scalar Multiplications	Total Number of Inverse operations	Protection against MIM attack	Computational Cost
ECDH	02	04	Nil	N	Medium
Ravi K Scheme	06	08	2	Y	High
Our Scheme	04	04	2	Y	Low

VII. Conclusion

The proposed scheme gives a comprehensive Access Control framework by leveraging computationally light Hash chains and Elliptical Curve Cryptography. Shared pair wise key have been derived by using Hidden Generator Points and is tied to the Node identities. This gives a safeguard against MIM attack eminent in ECDH. The Framework doesn't use any digital signature mechanism to achieve authenticated broadcasts. Instead secret value of hash chains has been used for the purpose. The framework can be embedded into any WSN based application where Entity authentication is a requirement.

References

[1] Akyildiz IF, et al. "A survey on sensor networks," IEEE Communications Magazine, 2002,40(8): PP. 102-114.

[2] Adrian Perrig, John Stankovic, David Wagner ," Security in wireless sensor networks" Communications of the ACM June 2004 vol 47,no. 6, pp 53-57.

[3] Xiaojiang.Du,Hsiao-Hwa.Chen,"Security in WSN," IEEE Wireless Communication August 2008.

[4] S.Mohammadi & H Jadidoleslamy ,"A Comparison of Link Layer Attacks on WSN," International journal on applications of graph theory in wireless Adhoc Networks & Sensor Networks ,Vol 3 ,No 1,March 2011 .

[5] Memsic,CrossBow Xserve User Manual May 2007.

[6] J. Hill et al., "System Architecture Directions for Networked Sensors, "ASPLOSIX: Proc. 9th Int'l. Conf. Architectural Support for ProgrammingLanguages and Operating Systems, New York: ACM Press, 2000, pp. 93-104.

[7] J. Hill et al., "System Architecture Directions for Networked Sensors,"SIGOPS Oper. Syst. Rev., vol. 34, no. 5, 2000, pp. 93-104.

[8] Andrea Zanella and Lorenzo Vangelista ,"Internet of Things for Smart Cities," IEEE INTERNET OF THINGS JOURNAL ,Vol 1,No 1, February 2014.

[9] D. Cuff, M. Hansen, and J. Kang, "Urban sensing: Out of the woods," Commun. ACM, vol. 51, no. 3, pp. 24–33, Mar. 2008.

[10] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz. "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," CHES2004,volume 3156 of LNCS, 2004.

[11] Xu Huang, et al. "Fast Scalar multiplication for Elliptic curve cryptography in Sensor Networks with Hidden Generator point," 2010 International conference on Cyber- enabled distributed Computed and knowledge Discovery.

[12] D. Hankerson et al,." Guide to Elliptic Curve Cryptography" Springer 2004.

[13] Bernard Menzes "Network Security and Cryptography," Cengage Learning.

[14] Arazi, B. (1999)." Certification of dl/ec keys,". In Proceedings of the IEEE P1363 Study Group for Future Public-Key Cryptography Standards.

[15] TinyOS. http:// www.tinyos.net.

[16] A. Liu and P. Ning et al." Tiny ECC: A Configurable Library for Elliptical Curve Cryptography in Wireless Sensor Networks," IPSN 2008.

[17] Lamport L.password "Authentication with insecure Communication,".Comm ACM 1981;24:770-772

[18] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," Ad Hoc Networks, Vol. 5, pp. 3-13, 2007.

[19] H. F. Huang, "A novel access control protocol for secure sensor networks,"Computer Standards & Interfaces, vol. 31, pp. 272-276, 2009.

[20] H. Huang, K. Liu, "A New Dynamic Access Control in Wireless SensorNetworks," 2008 IEEE Asia-Pacific Services Computing Conference, DOI 10.1109/APSCC.2008.116.

[21] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen and David E.Culler ," SPINS: Security protocol for sensor networks," proceedings of 7th International conference on mobile networking and computing, 2001, vol 8, no.5, pp 189-199 2001.

[22] S.,Setia,S., and Jajochia, S ,"LEAP: Energy efficient security mechanism for large-scale distributed sensor networks ," proceedings of the conference on computer and communications security ,03,ACM Press, Washigton DC, pp 62-72.76 2003.

[23] Karlof, C., Sastry, N., Wagner, D," TinySec: a link layer security architecture for wireless sensor networks ," Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, SenSys, Baltimore, MD, USA, November 3-5, 2004, pp. 162–175. ACM 2004.

[24] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn,and P. Kruus, "Tinypk, securing sensor networks with public key technology," Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and SensorNetworks (SASN 04), pp. 59-64, 2004.

[25] Youssou Faye,Ibrahima Niang and Thomas Noel ,"A survey of Acess Control Schemes in Wireless Sensor Networks," World Academy of Science ,Engineering and Technology Vol:5 2011-11-29.

[26] Moon A.H, Shah NA, Iqbal Ummer, Ayub Adil " Simulating and Analyzing Security Attacks in WSN Using Qualnet," IEEE Conference on ICMIRA,pp. 68-76.

[27] Ravi Kishore Kodali et al. "Implementation of ECC with Hidden Generator Point in Wireless Sensor Network,". 978-1-4799-3635-9/14 @2014IEEE.