A Survey of Access Control Schemes in Wireless Sensor Networks

Youssou Faye, Ibrahima Niang, and Thomas Noel

International Science Index, Computer and Information Engineering Vol:5, No:11, 2011 waset.org/Publication/3624

Abstract—Access control is a critical security service in Wire- less Sensor Networks (WSNs). To prevent malicious nodes from joining the sensor network, access control is required. On one hand, WSN must be able to authorize and grant users the right to access to the network. On the other hand, WSN must organize data collected by sensors in such a way that an unauthorized entity (the adversary) cannot make arbitrary queries. This restricts the network access only to eligible users and sensor nodes, while queries from outsiders will not be answered or forwarded by nodes. In this paper we presentee different access control schemes so as to ?nd out their objectives, provision, communication complexity, limits, etc. Using the node density parameter, we also provide a comparison of these proposed access control algorithms based on the network topology which can be flat or hierarchical.

Keywords—Access Control, Authentication, Key Management, Wireless Sensor Networks.

I. Introduction

SENSOR nodes in WSNs are short-range radio communication capabilities. WSNs are being deployed for a wide variety of applications, including military sensing and tracking, environ- ment monitoring, patient monitoring, etc. They have some unique characteristics such as large scale of deployment with large number of sensor nodes. Each node has constraints on resource such as energy, memory, computation speed and bandwidth. Many factors like deployment nature in hostile environment, wireless communication, the physical interactions with the environment, and other objects make WSNs more vulnerable to various attacks. Thus, access control become a very challenge. It de?nes policies that entities (base station, sensor nodes or users) join and/or queries the WSN. In general, the collected data may not be so critical, such as the query of the current temperature in a location within a building. However, in WSNss critical applications, the collected data and secrets should be protect by preventing unauthorized users from gaining the information. Data in real-time WSNs applications are made available to users on demand. Data may no longer be accessed only at the base station or a gateway node. They could be accessed anywhere from a sensor node in an ad-hoc manner [1].

Note that, access control becomes especially difficult in presence of node capture, query replay and denial of service (DoS) attacks. In hostile environments, not only sensor nodes but also users may be compromised by adversaries. Node capture means gaining full control over a sensor node by a physical attack. User capture means the attackers can disguise themselves into legitimate users to use network resources and attack the networks.

Authenticated packets which are sent over a multi-hop connection using only symmetric cryptography is challenging because the intermediate nodes that forward the packets may also have the symmetric key used for authentication (they need this key to be able to authenticate the packet). An attacker that captures a node will get access to the symmetric key. Thus, security solutions in this domain cannot rely on single sensor.

There are tree types of general access control: new node addition schemes, user authentication schemes and authenticated querying. Based on network topology and node density parameter, we provide a comparison between these schemes.

The reminder of the paper is setup as follows: background is presented in section II. Section III and IV present respectively access control challenges and access control schemes. We conclude with future works in section V.

II. Background

A. Security Vulnerabilities in WSNs

Sensor networks possess a large number of vulnerabilities which makes them even more prone to attacks. We distinguish physical vulnerabilities and technological vulnerabilities.

1) Physical vulnerabilities: Due to the deployment nature (in public and hostile environments) renders more link attacks ranging from passive eavesdropping to active interfering, sensor nodes would be highly vulnerable to capture and vandalism. WSN can scale up to thousands of sensor nodes without any fixed infrastructure. This implies the need to develop simple, flexible, and scalable security protocols. And new nodes addition and failure make the network topology dynamic and the solutions more complex.

2) Technological vulnerabilities: Security services in WSNs must consider the hardware constraints of the sensor nodes:

- *Energy*: energy consumption in sensor nodes can be categorized into three parts: energy for the sensor transducer, energy for communication, energy for microprocessor computation.
- *Computation*: sensor nodes's processors are not generally powerful such as complex cryptographic algorithms cannot be used in WSNs.

Y. Faye is with the Department of Computer Science (Laboratory LIFC) ,University of Franche-Comte, Besanon, FR, 25000 France (phone:+33.3.81.66.20.78; +33.6.37.04.95.49; e-mail:yfaye@lifc.univ-fcomte.fr).

I. Niang is with the Department Mathematic and Computer Science (Laboratory LID), Cheikh Anta Diop University, Dakar, Senegal (e-mail: iniang@ucad.sn).

T. Noel is with the Department Mathematic and Computer Science (Laboratory LSIIT), Strasbourg University, Strasbourg, France (e-mail: see noel@unistra.fr).

- *Memory*: there is usually not enough space to run complicated algorithms after loading OS and application code.
- *Transmission range*: the communication range of sensor nodes is limited both technically and by the need to conserve energy. The study in [48,49] found that each bit transmitted in WSNs consumes about as much power as executing 800-1000 instructions. Thus, communication is more costly than computation in WSNs.
- *Wireless communication*: its characteristics make traditional wired-based security schemes unsuitable. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications.

B. Key Management in WSNs

Key management consists of key establishment, key revocation and key update. It is a big challenge in sensor networks because the nodes may not know anything about their neighbors before deployment. There are four types of general key agreement schemes: the *trusted-server scheme,* the *self-enforcing scheme*, the *key pre-distribution scheme* and *no key pre-distribution scheme*. The *trusted-server scheme* depends on a trusted server for key agreement between nodes. This type of scheme is not suitable for sensor networks because there is usually no trusted infrastructure in sensor networks. The *self-enforcing scheme* depends on asymmetric cryptography, such as key agreement using public key certificates. Public-key cryptography provides a more flexible and simple interface requiring no key pre-distribution, no pairwise key sharing, no complicated one-way key chain scheme. However, limited computation and energy resources of sensor nodes often make undesirable to use public key algorithms . The third type of key agreement scheme is *key pre-distribution*, where key information is distributed among all sensor nodes prior to deployment. Cryptographic algorithms require keys to be shared between entities (sensor nodes, base station and user). We classify key pre-distribution schemes as probability schemes and determinist schemes.

1) Determinist key pre-distribution scheme: Determinist approaches guarantee that any two intermediate nodes can share one or more pre-distribution keys. The key distribution is determined by the pattern communication of protocol used, that is, which nodes share a secret key. There are different types of determinist key pre-distribution schemes in sensor networks, including single network-wide keying, pair-wise keying and groups keying[44,45,50].

2) Probabilistic Key Pre-distribution: For large networks, a probabilistic method is more efficient than a deterministic method. In this scheme, the existence of one or more common pre-distribution keys between intermediate nodes is not certain but is instead guaranteed only probabilistically. The basic idea of these schemes is to randomly preloaded each sensor with a subset of keys K from a global key pool P before deployment. A common key in both key rings of a pair of nodes is used as their pair-wise key. It guarantees enough resilience even though not perfect resilience, because the probability of breaking communication link is *k/P*. Moreover, it supports the large scale networks [46].

3) No Key Pre-distribution: Contrary to most of key management using pre-loaded initial keys, this mechanism is considering the reality of wireless sensor networks. If an adversary does not know where and when nodes are deployed, it is difficult to launch active attack at an early phase. In Key infection scheme, key setup is completed in a relatively short time through a few transmissions [47]. That different from key pre-distribution schemes, no pre-distribution key is stored in sensor nodes. This type of schemes establishes secure link keys by broadcasting plaintext information first. The advantage in this mechanism is that it consumes relatively less energy. Unlike the pre-distribution schemes above, it need not load potential keys into a node, which results in the low cost of network organization. However, it is only strong when an adversary does not observe communication during key setup, and it cannot add nodes since a pair-wise key is established through exchanged data during key setup.

III. Access Control Challenges

A. Sensor Network Architecture

A WSN is large number of sensors distributed over a sensor field using one or a more base stations. In this case, all sensor nodes trust the base station. In this paper, for better studying access control, we consider two types of wireless sensor network as illustrated in Figure 1 and Figure 2. In the Figure 1, we show a WSN which offers services to mobiles users. Base station serves as access point for network administrator and management of security services. Sensor nodes are the access points for user (laptop, PDA, mobile phone) to data in the WSN. Only authorized users have to access the WSN's data, e.g., they have subscribed to a "WSN's data service". Figure 2 shows a WSN without connected users. Examples of such WSN applications are time-driven application or event-driven application. Only the base station should be allowed to send queries. In this case, to prevent the adversary from querying the network, an access control mechanism should be built into each sensor node. From the above architectures, we distinguish two levels of access control: *Inside access control* and *Outside access control.*

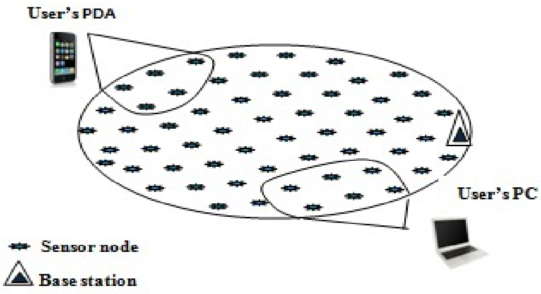

Fig. 1. WSN's outside access control architecture.

Inside access control: refers to secure communication between sensor nodes and communication between sensor nodes and base stations. It involves the two above architectures.

Outside access control: means secure communication between the WSN (sensors nodes and base station) and the

International Science Index, Computer and Information Engineering Vol:5, No:11, 2011 waset.org/Publication/3624

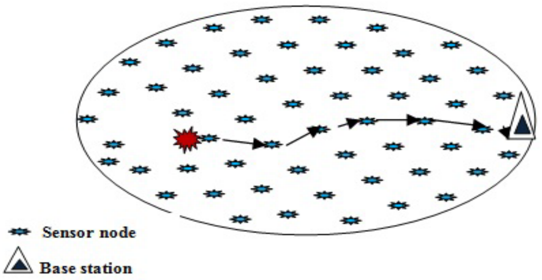

Fig. 2. WSN's inside access control architecture.

outside users. An authorized user can send data requests to some sensor or a set of sensors in her neighborhood. Only Figure1 is involved.

B. Access Control Services

Access control in WSNs can be divided in two services: *Authentication* and *Authorization*.

1) Authentication: Means establishing a relation between the user and some identity. An identity is the individuality property of a user which ideally cannot be forged or copied.

Authentication can be classify on: *user authentication* and *authenticated querying*. In *user authentication*, the user sends his name and proofs of his identity to a sensor node, and the sensor should be able to decide whether or not the identity is valid and in fact belongs to the user of that name. *Authenticated querying* provides if a query comes from an authorized user, a base station or a sensor node. A WSN provides *authenticated querying* if it satisfies the following properties (perhaps, with some probability):

- *Safety*: if a sensor node in WSN accepts a query as a legitimate query, then this query was originated by WSN or posted by an authorized user.
- *Liveness*: any legitimate query will be received by all sensors in WSN which must process it in order to give the required answer to the legitimate entity. That limits the propagation of a fake query.

2) Authorization: Means establishing a relation between a user and a set of privileges (access rights or allowed operations). In this service, a user sends his name together with the requested access operations (e.g., read, write) to a sensor and the sensor should be able to decide whether or not this user is allowed to perform this operation.

Note that, for access control schemes, authentication user or authenticated querying and authorization can be combined into one single operation. If a request is sent, the access control mechanism checks legitimacy (authentication and authorization), and sends a response back to the user (which may be the data requested or a message "access denied").

IV. ACCESS CONTROL SCHEMES IN WSNs

Many access control algorithms are proposed, we distinguish: *new node addition schemes*, *authenticated querying* and *user authentication schemes*.

A. New Node Addition Schemes

To prevent malicious nodes from joining the sensor networks, access control is required in the design for controlling sensor node deployment. Since sensor nodes are highly constrained in terms of resources and can be deployed in hostile environment, they may be lost because of power exhaustion or malicious attacks. Therefore, new node deployment is necessary. Schemes based on elliptic curve cryptography (ECC) [19, 20] are proposed. Some of them are static[6,7,8,9] and other dynamic because all the old secret keys and broadcasting information in existing nodes should not be updated once a new node is added. In the rest of this paper, we present only dynamic mechanisms.

In [2], a secure network access system is presented. It provides node authentication, packet authentication, packet integrity, packet confidentiality. Also, this solution uses Self-Certified Elliptic Curve Diffie-Hellman (ECDH) cryptosystem [3] to establish a pairwise key between a new sensor node and a controller node *c*. Thus, they need to have a Certificate Authority *(CA)*, and controller nodes witch can be a regular sensor nodes or a more powerful nodes. These controller nodes launch a two-way authentication with new node and establish a pairwise key using Self- Certified ECDH protocol.

To avoid possible DoS attacks against the Self-Certified ECDH protocol, a polynomial-based weak authentication scheme [4] is first developed. The Certificate Authority *(CA)* first generates a bivariate *t*-degree polynomial *f* over a finite field *GF(p)*, where *p* is a large prime number. Function *f* satisfies the following property: *f(x,y) = f(y,x)*. For a controller *c*, the *CA* evaluates *x* in the bivariate polynomial *f(x,y)* by *c*, and deploys *f(c,y)* onto c. For regular node *i*, *CA* evaluates *x* in *f(x,y)* by *i*, and deploys *f(i,y)* onto *i*. When node *i* and controller *c* want to communicate each other, they can establish a pairwise key based on each other's *ID* since *f(c,i) = f(i,c)*. Then they can use key *f(i,c)* to authenticate the exchanged messages.

Before a new node *i* joins a group in the WSN, the *CA* first generates and distributes private keys and related parameters to all nodes in the network, including controller nodes and regular sensor nodes. Controller nodes periodically broadcast their identity (ID_c). The new node *i* picks a controller node with the strongest signal strength (RSSI) and sends a request message to the controller node. This request message contains its Self-Certified ECDH public key U_i, nonce (number once), and it's ID_i. Node *i* also appends a HMAC using the pairwise key k_{ic} generated by the polynomial scheme. Once the controller node receives this request message, it evaluates polynomial share using *i*, derives the key k_{ci}, and verifies the HMAC. If the HMAC is not correct, it simply drops the request message. Otherwise, the controller node performs Self-Certified ECDH to establish a pairwise key, sk_{ci}, with node *i*. Next, it sends back a reply message containing its Self-Certified ECDH public key U_c with one HMAC using k_{ci} and a new HMAC using sk_{ci}. After some random delay, controller node *c* sends out the new group key encrypted by using key sk_{ci}. At this time, node *i* should have finished its Self-Certified ECDH operations and obtained k_{ic}. Then node *i* decrypts new group key and configures its radio to use the new group key.

For an access control, all nodes in the group will use the same group key to protect packets transmitted in wireless sensor networks. On the sender side, the sending node generates a message integrity code (MIC) for each outgoing packet using the group key. On the receiver side, the receiving node uses the group key to verify the MIC included in each incoming packet. If the MIC can be verified, the receiver forwards the received packet up in the radio stack. Otherwise, the receiver simply discards the packet.

However, the security of this scheme depends on that of key distribution mechanism which it is based. All eligible nodes share a network-wide key. When one node is compromised, the secret key must be update. Some mechanisms [2, 43, 44] are used to update the secret key. Note that, the secret of the polynomial is weak, if a number of node higher than polynomial's degree are compromised the secret polynomial is disclosed. Therefore, it can only provide weak authentication, and cannot replace Self-Certified ECDH to establish secret keys. Solutions using others mechanisms are described below.

A Novel Access Control Protocol for Secure sensor networks(NACP) proposed in [5] is based on elliptic curve cryptography (ECC) and Hash chain. It has a very simple and efficient authentication procedure and common key generation, and also is quite adequate for power and resource constrained sensor nodes. NACP is based on Zhou et al. solution [10] which proposed an access control protocol based on ECC for sensor networks that is more efficient than those algorithms based on RSA [11]. Zhou et al. scheme allows a new node to join the sensor network dynamically, and key establishment is also included in access control protocol to help the new node establish shared keys with its neighbors so that it can carry out secure communications among sensor nodes. It also included a timestamp to provide authentication procedure. However, Zhou et al. scheme also assumes that each sensor node can sustain a tolerance time interval before it is compromised [10, 12]. Then, it will be not convenient for some practical implementations in sensor networks.

A New Dynamic Access Control Protocol (NDACP) is proposed in [13]. It is also based on Zhou et al. scheme. This solution controls a new node joining sensor network and uses hash function which is very suitable for power and resource constrained sensor nodes. In the proposed protocol, every node needs to perform only five hash function computations, four exclusive-OR (XOR) operations to accomplish mutual authentication, and a shared key establishment for secure communication. It is very adoptable for the sensor nodes.

NACP uses the same approaches than [13]; it does not require a timestamp or a sustaining tolerance time interval for each node. It can be used more conveniently for practical implementation. It could reduce large amounts of computations and communications between two nodes. NACP accomplish two tasks: *node authentication* and *key establishment*

Node authentication: a deployed node establishes its identity with its neighboring nodes and it has the right to access the sensor network through authentication.

Key establishment: through authentication, shared keys should be created between a deployed node and its neighboring nodes to provide secure communication. This guarantees that any two sensor nodes can find a common shared key between themselves. This shared key is a pairwise key. NACP has three phases: *initialization phase*, an *authentication* and key *establishment phase*, and *new node addition phase*.

Initialization phase: let us assume there are a number of neighborhood N_1,N_2, ...,N_r with in a designated area. Base station first chooses *r* secret keys k_1, k_2, ..., k_r and pre-loads each secret key k_i and a one-way hash function *h()* to its corresponding node N_i. Base station computes hash chain $h^z(k_i)$ = h($h^{z-1}(k_i)$) and broadcasts the commitment $h^z(k_i)$ and the number *z*, where *z* is a large constant number.

Authentication and key establishment phase: after nodes authenticate each other with hash chain, they share a common key (hereafter a pair-wise key) together. Suppose a node N_i and a node N_j are neighborhood. N_i and N_j's current hash chains are $h^{z-u}(k_i)$ and $h^{z-v}(k_j)$, respectively. Authentication and key establishment phase is as below.

1) N_i generates a random number t_i and computes the point $A_i = t_i$P = (Ax_i,Ay_i) over the elliptic curve E_q and s_i = h(Ax_i $\|$ $h^{z-u-1}(k_i)$). N_i broadcasts A_i, s_i,N_i. N_j also generates a random number t_j and broadcasts A_j, s_j,N_j where $A_j = t_j$P = (Ax_j,Ay_j) and s_j = h(Ax_j $\|$ $h^{z-v-1}(k_j)$).
2) N_i computes $K_{ij} = t_i A_j$ = (Kx_{ij},Ky_{ij}) and z_i = h(Kx_{ij} $\|$ $h^{z-u-1}(k_i)$) and then broadcasts z_i, $h^{z-u-1}(k_i)$. N_j verifies h($h^{z-u-1}(k_i)$) = $h^{z-u}(k_i)$. If it is valid, N_j computes $K_{ij} = t_j A_i$ = (Kx_{ij},Ky_{ij}) and checks whether h(Ax_i $\|$ $h^{z-u-1}(k_i)$) = s_i and h(Kx_{ij} $\|$ $h^{z-u-1}(k_i)$) = z_i. If it holds, then N_j authenticates N_i as a legal node.
3) N_j also computes z_j = h(Kx_{ij} $\|$ $h^{z-v-1}(k_j)$) and broadcasts z_j, $h^{z-v-1}(k_j)$.
4) N_i also verifies h($h^{z-v-1}(k_j)$) = $h^{z-v}(k_j)$ and checks whether h(Ax_j $\|$ $h^{z-v-1}(k_j)$) = s_j and h(Kx_{ij} $\|$ $h^{z-v-1}(k_j)$) = z_j . If it holds, Ni also authenticate Nj as a legal node.
5) N_i and N_j update their hash chain to be $h^{z-u-1}(k_i)$ and $h^{z-v-1}(k_j)$ and inform all the group of nodes by using the base station, respectively.

New node addition phase: when a new node with identity N_{r+1} is added, base station also generates a secret key k_{r+1} and hash chain $h^z(k_{r+1})$ and pre-loads k_{r+1} to the new node N_{r+1}. Similarly, base station informs $h^z(k_{r+1})$ and *z* in networks. Authentication and key establishment are performed as the above. Node addition is available until a node consumes all the values of its hash chain.

However, in [14], it is show that NACP is insecure to the replay attack and against new node masquerading attack in the presence of an active adversary due to the absence of authentication method for the base station. Only unilateral authentication is provided. NACP has also the lack of hash chain renewability, which is one of the necessary aspects in the sensor network with memory restricted nodes. To cope with, a Enhanced Novel Access Control Protocol (ENACP) [14] which is quite adequate for power and resource constrained sensor networks is proposed to solve these problems by supporting the mutual authentication and adding a renewal of hash chain phase for the renewability of the hash chain.

TABLE I
COMPARISONS OF COMPUTATION AND TRANSMISSION FOR SOLUTIONS.

Scheme	Computations for each node to achieve authentication and compute a common key	Total number of transmissions for the protocol to establish key
Zhou et al.[10]	$3T_{EM}$+T_i+T_H	21
NACP[5]	$2T_{EM}$+ $5T_h$	10
ENACP[14]	$2T_{EM}$+$8T_H$	14
PACP[15]	$2T_{EM}$ + $5T_H$	8
NDACP[13]	$5T_H$	7

T_{EM}: point multiplication over an elliptic curve,
T_i : the time for one modular inverse computation
T_H : time for executing the adopted one-way hash function in one's scheme. Note that the time for computing modular addition and XOR operations is ignored, since they are much smaller than T_{EM}, T_i, and T_H.

In a Practical Access Control Protocol for Secure Sensor Networks (PACP) [15], some weakness are also identified and point out NACP in two sides: network-lifetime and availability. Network lifetime is limited according to the size of the hash chains. Because N_i has no way to authenticate itself to neighborhood after it uses $h^{z-z+1}(k_i)$. That is, this scheme is not still dynamic access control in a broad view. Second, authentication by hash chain requires huge communication overhead and memory cost.

According to NACP, base station is responsible for announcing the updated hash chains. It means that, nodes have to inform node's state to base station, normally through multiple hops. In addition, after base station broadcasts the updated hash chain, each node has to store node's state because any node cannot know who will next request to authenticate. In [15], the access control mechanism support NACP security and exploits just hash operation, not hash chain. It does not need to inform the state of hash chain and it is enough to perform a single hash function.

In [16], some inherent flaw are identified in the design on [14] and demonstrated that in the new node injecting and hash chain renewal phases, the protocol is vulnerable to a new node masquerading and a legal node masquerading attack, in violation of their security claims. With regard to efficiency and communications, these schemes are compared in Table I.

B. Authenticated Querying

Query authentication implies data origin authentication and data integrity. To separate concepts we distinguish user's query and system's query. User's query namely *outside authenticated querying* means queries sent by a user to a WSN. System's query namely *inside authenticated querying* means base station's queries or sensor nodes queries. Most sensor nodes will not receive the query directly from the base station, but from another sensor. Therefore query authentication is needed to ensure that data send by the sensors correspond to the original query. In this case, to prevent the adversary from querying the sensor network, an access control mechanism should be built into each sensor node. We review some of works on authenticated querying in WSNs.

1) Outside authenticated querying: WSN satisfies user authenticated querying if it satisfies the following properties:

Safety: if a sensor *s* processes a query *q*, then *q* was posted by a legitimate user.

Liveness: any query *q* posted by a legitimate user will be processed at least by one or each sensor of the set of sensors which must process the query in order to give the required answer to the user.

a) Realizing robust user authentication

Zinaida Benenson et al. [17] realized robust user authentication which is a threshold solution to the node capture attack. This means if the number of sensor nodes in user's communication range is *n*. Of these, *t* (*t*<*n*) sensors are allowed to fail or to be malicious, meaning that they are captured and run programs which are different from the expected ones. Therefore, the user can rely for communication on at most *n-t* sensors in his communication range. Benenson et al. scheme provides authenticated querying for WSNs when the user's query involves only a single sensor node, e.g., "the temperature sensed by the sensor *s*".

The natural method to use for authentication of a large number of users is public key cryptography because of its scalability. The basic idea of this scheme is to let the sensors in the communication range of the user serve as interpreters (or a gateway) between the public key cryptography of the user and the symmetric cryptography of WSNs. So the sensors should communicate with each other using symmetric cryptography. The user authenticates itself to the sensor nodes in its communication range using public-key cryptography and after that these nodes communicate with the rest of the sensor network on behalf of the user using symmetric cryptography. This approach uses a Public Key Infrastructure (PKI) with a different certificate management strategy. The base station acts as a central Certificate Authority (CA), i.e. CA (priv_keyCA, pub_keyCA). A legitimate user certificate (U) is signed by the CA with user public key, i.e. certU = signCA(pub_keyU). Each sensor node is also pre-loaded with public keyCA, so that each of them can independently verify user certificates.

Since public key cryptosystems [18, 19] require more overhead for decryption and signature generation which are slow and resource-demanding than encryption and digital signature verification. Therefore, these cryptosystems can be used in sensor networks only if the sensors are not required to decrypt or to sign messages. In contrast ECC requires more overhead for encryption and signature verification than for decryption and signing and is still feasible for sensor nodes.

In a first step of Benenson et al. solution, the user unilaterally authenticates to the sensors in his proximity using public key cryptography, and sensor nodes run only digital signature verification. However, it could possibly become a bottle neck for sensor nodes to perform the verification process during a high traffic load of the whole network. Note that, sensor nodes do not authenticate to the user, a single captured sensor node could impersonate many valid sensor nodes and authenticate the adversary. However, in a fully implemented solution to authenticated querying, sensor nodes also authenticate to the user, and append some information to the query such that other sensors can verify the legitimacy of the query. ECC can be chose for implementation of robust user authentication with mutual authentication and session key establishment as a full solution in future work according to the authors.

This scheme can be vulnerable to jamming attack in MAC layer, by broadcasting several bogus certificates. It is very restrictive and does not scale well for queries which need data from a set of sensor nodes, e.g., calculating the average temperature over a given region.

b) Symmetrical key based access control

Symmetrical key based access controls are few in WSNs. Benenson et al [17] is the first scheme provides authenticated querying for WSNs when the user queries involve only a single sensor node. In that sense, their scheme is very restrictive and does not scale well for queries which need data from a set of sensor nodes. Proposed by Satyajit Banerjee et al. [21], Symmetric Key Based Authenticated Querying improvises on the pairwise key pre-distribution technique of Blundo et al [22] and relies on it to additionally support authenticated querying. It is a threshold scheme for authenticated querying in WSNs when user queries involve multiple sensors . In addition it is fully symmetric key based.

Like [17], the authors deal only with the safety property of authenticated querying in WSNs and expect some other protocol (e.g. secure routing) to handle liveness property separately and complement the scheme. The scheme is based on randomly symmetric bivariate polynomial which acts like a global secret

A user starts the protocol by broadcasting its identity ID_u and the query q in the WSN. On receiving q and the ID_u, the WSN identifies the set of sensor nodes S_q which must process the query q. These sensors in might, elect a leader amongst themselves using method described in [23], and the leader takes the responsibility to randomly generate a nonce and transmit to all other sensors in S_q. Then, the user is notified about S_q and the nonce. For each sensor in S_q the user computes a MAC and forms the collection of all the MACs and sends it back to each sensor in S_q. Each sensor in S_q, upon receiving the collection of MACs computes the MAC on the challenge nonce. Thus, the node verifies whether MAC belongs to the collection of MACs received. If a matching MAC is found it participates, else it drops out from the process.

Since this scheme relies on the pairwise key pre-distribution scheme of Blundo et al., it is perfectly secure up to *(t-1)* number of node or user captures, where (t is the degree of the bivariate polynomial used).

Compared with Benenson et al. [17], this scheme has many advantages:

- It is fully symmetric key based as opposed to the mixed approach of both public and symmetric key cryptography.
- It relies on the perfect security of the underlying key pre-distribution scheme and their scheme relies on the provable security of the elliptic curve based certificate scheme.
- It considers queries involving multiple target nodes.

However, the scheme is not full proof against DoS attack. An adversary can inject bogus messages and keep nodes busy in unnecessary processing. Though the adversary does not succeed to authenticate herself, he/she can cause potential dissipation of the battery power of the nodes. To get rid of such problem, the scheme needs to support some mechanism that ensures early rejections of illegitimate queries.

c) Usage of the one-way key chain and Merkle ash tree for authenticated querying

The usage of the one-way key chain and the Merkle hash tree have advantages over the current access control methods. They are low expenses in calculation, storage and communication, and are several resistance to node capture, query replay and DoS attacks.

single key chain based access control scheme: a single key chain based access control scheme allows only one user to visit the network simultaneously because of using a single key chain. This limitation can be solved by the method of multiple key chains based on access control scheme[53]. In a single chain based access control, to generate the one-way key chain of length *n*, the central server or base station chooses the last key K_n randomly, and generates the remaining values by successively applying a one-way function *F*: K_j=*F*(K_{j+1}), *0≤j<n*. Because *F* is a one-way function, anybody can compute forward, e.g. compute K_0,...,K_j given K_{j+1},but nobody can compute backward, e.g. compute K_{j+1} given only K_0,...,K_j. Each node is pre-distributed with the chain commitment K_0 before it is deployed.

A user who needs to access the sensor networks firstly apply for a key sequence from the base station. The central server first distributes the key chains which are made of keys with small index. If the key chain which user got is K_n,...,K_m, *n<m*, this means the user can send at most *m-n+1* queries to the networks (a key is used when sending a query).

The sensor nodes which received query q authenticate K_i (key use with query q) through proving whether i>j, K_j =$F_{i-j}(K_i)$ holds, of which K_j is the authentication key stored by sensor nodes. If the authentication is passed, it proves that this query is legitimate, the nodes respond to the query and replace K_j with K_i, otherwise reject the query.

Mechanisms using one way key chains have several advantages: they use symmetric key and resist against DoS attack. Note that, the security of the one-way key chain based access control scheme depends on that of one way pseudo-random function. The sensor nodes can authenticate query on receiving it. As a result, they are immune to the DoS attacks.

Merkle hash tree based access control: to further increase the flexibility of the key chain based access control and lower the storage expenses of nodes, a Merkle hash tree is proposed to authenticate and distribute these key chain commitments. In Merkle hash tree, the base station pre-computes *m* (*m* the number of key) one-way key chains, each of which is assigned a unique integer-valued between 1 to *m*. The central server computes K_i=h(C_i) for all i∈1,...,*m*, and constructs a Merkle tree using K_1,...,K_m as leaf nodes. C_i denotes the commitment of the *i-th* key chain and *h()* a hash function. Specifically, K_1,...,K_m are arranged as leaf nodes of a full binary tree, and each non-leaf node is computed by applying *h()* to the concatenation of its two children nodes.

The base station constructs a commitment distribution certificate for each key chain. The certificate for the *i-th* key chain consists of the set C_i and the values corresponding to the siblings of the nodes on the path from the *i-th* leaf node to the root in the commitment distribution tree.

The base station distributes the key chain and the corresponding commitment distribution certificate to each user and also pre-distributes the root of the commitment distribution. When a user needs to access WSNs, it broadcasts the commitment distribution certificate. Each sensor can immediately authenticate it with the pre-distributed root of the parameter distribution tree. As a result, all users can use this key chain to access the WSNs.

In Merkle hash tree, it is not necessary for sensor nodes to store information of the commitments for each key. The sensors only need to store the root of the Merkle hash tree and the commitments being used in the network, instead of all the key chain commitments. Each key in the one-way key chain is used only to send a query. The scheme can resist the attacks of the query information replay. The attacker capturing the nodes has no effect on the security of the access control scheme. When the users are captured, the attacker obtains the key chains used by the users and can disguises selves into the legitimate users to send queries to the network. To increase scalability of Merkle hash tree based access control scheme, multi-layer Merkle hash tree are introduced in [53].

Table II describes the comparison schemes for user authenticated querying using two parameters: communication complexity witch depends on nodes density and storage complexity. *u* denote the number of key chains being used, *n* the number of sensors which must successfully authenticate the legitimate, *t* the degree of polynomial which is used to negotiate keys and *N* the number of sensor nodes in the WSN.

TABLE II
COMPARISON OF USER AUTHENTICATED QUERYING SOLUTIONS.

Solutions	Communication Complexity	Storage Complexity
Single Key Chain based access control	O(1)	2
Merkle hash tree based access control	O(1)	2+2xu
Realizing robust user authentication	O(n)	2
Symmetrical key based access control	$\sqrt{N}$	O(tlog(N))

2) Inside authenticated querying: WSNs's data may be valuable or critical, it should be protected from the unauthorized access. In particular, only the base station should be allowed to send queries. In inside authenticated querying, the safety and liveness properties are defined follow:

Safety: If a sensor node in WSN accepts the query *q* as a legitimate query, then *q* was originated by the base station.

Liveness: any legitimate query *q* will be received by all sensor nodes in WSN.

Some approaches to authenticated broadcast in sensor networks exist. Zinaida Benenson et al. proposed authenticated query flooding in sensor networks [24]. This scheme consider how the base station can authenticate its queries, such that only legitimate queries are answered by sensor nodes while propagation of fake queries is probably restricts to a logarithmic part of the network . This protocol uses only symmetric cryptography. It is based on the ingenious protocol proposed by Canetti et al. [25], but it has a much better performance, as it relies on the implicit cooperation between sensor nodes which occurs when the authenticated query is flooded into the network.

The author assumes that an ID-based key pre-distribution scheme [26, 27] is deployed in the sensor network. It uses the *pass strategy*, that's mean, if the sensor cannot decide whether the query is legitimate or not, it passes it to its neighbors. It is a probabilistic query authentication protocol that uses 1-bit MACs after apply on a query *q* a hash function *h().*The idea of using MACs with single bit output originates from [25]. In this protocol each sensor node is preloaded with keys chosen randomly from a large key pool, and for each query, a number of 1-bit MACs are computed using keys chosen from the same key pool. When receiving a query, the sensor node has, with some probability, some of the keys used to calculate the 1-bit MACs and can verify the authenticity of the query. To increase the chances of discovering a fake query, the number of 1-bit MACs has to be large, resulting in increased message length. The query of a legitimate user will be flooded into the sensor network without any obstacles. However, a query forged by an adversary will only be able to reach a limited part of the network, as some sensor nodes will discard the query. It is infeasible for an adversary to first choose some number *x* and then search for an appropriate value of query q with *h(q)=x*.

Some other approaches to authenticated querying broadcast in sensor networks exist in the literature.

In a Security Protocols for sensor Networks (SPINS) [28], authenticated streaming multi-cast μTESLA is realized using one way hash chains, time synchronization and a symmetric keys shared by the base station with each sensor in the network. It can be used for query authentication. The protocol achieves asymmetry by a delayed disclosure of the symmetric keys and uses MACs to authenticate the broadcasted messages. μTESLA is a very efficient protocol. Its security depends on the security of the underlying time synchronization mechanism. However, devising a protocol which globally synchronizes time in a large sensor network seems to be a difficult problem [29].

Relatively inexpensive digital signatures can also be used for authenticated flooding (see, e.g., [30]), assuming that each sensor node is preloaded with the public key of some certification authority. However, these signatures are still very expensive considering the limited resources of sensor nodes.

C. User Authentication

User authentication (UA) is a basic solution used for access control issue. Many examples of measures can be found in our daily life, such as login to our office's local area network, down to a password-based authentication for our account transactions on banks etc. A review of current studies on WSN reveals that user authentication has not been adequately addressed due to the resource-constrained nature of WSNs.

Traditional UA solutions are quite interesting to examine various works on smart cards based on UA schemes for mobile communications or remote networking environments.

Password-based authentication schemes are the most widely used techniques for remote user authentication. Many static ID-based (based on static login ID) remote user authentication schemes both with or without smart cards have been proposed [31,32,33,34, 35]. Most of them do not allow the users to choose and change their passwords. They maintain a table to verify the validity of the user's login. Other schemes [37] are based on dynamic login identity (ID) to avoid the risk of ID-theft. These solutions use a one-way hash function to resist attacks like replay attacks, forgery attacks, guessing attacks and insider attacks. They can be categorized into two types: some of them use weak-password and the other use strong-password. Note that, weak-password authentication scheme is based on public-key cryptographic techniques and has the advantage that the remote system does not need to keep a table for verify and is easy to memorize. However, weak-password authentication schemes lead heavy computational because of using public-key cryptographic. It cannot be applied to a WSN environment. In contrast, the computational load of most strong-password authentication schemes is lighter because of using only simple operations (e.g., one-way hash function [36] and exclusive-OR operation). The strong-password authentication schemes have another advantage over weak-password authentication schemes, that their implementations are easier and with less cost. However, a strong-password is difficult to memorize. Additionally, the strong-password authentication schemes suffer from stolen verifier attacks and guessing attacks.

It is difficult to apply traditional UA solutions in WSNs. There has not been much work published on.

The Usage Control based Security Access Scheme for Wireless Sensor Networks (UCON) [52] model is introduced as the next generation access control model. UCON extends traditional access control to consider the problem of authorization not only at the time of access to a resource but also during its usage. The most important properties that distinguish UCON from traditional access control models are the continuity of usage decisions and the mutability of attributes.

In the rest of this paper, we study the UA problem in WSN where legitimate user is allowed to query and collect the data at any sensor node of the network. We note that, some strong-password based solutions are proposed to resolve access control problem in WSNs.

Wong et al. [39] proposed a lightweight strong-password based on dynamic user authentication protocol. This scheme allowed authorized users to access the network anywhere using mobile devices. It uses basically one-way hash function and exclusive-OR operation to provide the dynamic user authentication like [38]. Wong et al. claim that, their scheme can resolve forgery attacks, replay attacks, and modified login message attacks.

Wong et al. solution consists of three phases: *Registration phase*, *Login phase*, and *Authentication phase*. We briefly describe the operation of this protocol below.

1) *In Registration phase:* a user submits his/her identification (ID_u) and password (PW) to the gateway node (GW-node). The GW-node computes some values A and B. The GW-node replies to the user for successful registration and stores these values along with ID_u and PW. The GW-node distributes ID_u along with A and timestamp (T_S) to those sensor nodes, which are able to provide a login interface to users namely login node.
2) *In Login phase:* a user submits his ID_u and PW to a login node witch checks the validity of the ID_u. If true then the login node retrieves the A and computes not only B but also authenticators C_2 and C_1. The login node then sends ID_u along with C_2, C_1 and current timestamp (T) to the GW-node for final authentication process.
3) In *Authentication phase:* the GW-node checks the validity of the user ID_u and the timestamp. If both are valid, then the GW-node retrieves corresponding A and B and computes C_2 and C_1. To valid the authenticators, an accept message is sent to the login node which is forwarded to the user

However, some works [40, 41, 42, 51] show that Wong et al. scheme is vulnerable to the replay and forgery attacks. For this, user cannot change his/her password freely and cannot also prevent replay attacks. To solve this problem, Tseng et al. [40] proposed a lightweight dynamic user authentication scheme for WSNs. There approach not only retains all the advantages in Wong et al. scheme but also enhances its security by withstanding the security weaknesses and allows legitimate users to change their passwords freely. The proposed scheme is divided into four phases: *Registration phase*, *Login phase*, *Authentication phase*, and *Password-changing phase*. The authors claimed that their scheme possesses many advantages, including resistance of replay attack, forgery attacks, reduction of user's password leakage risk. It has the capability to change password, and propose better efficiency.

But, in [41], Vaidya et al. show that, the solution in [40] has security weaknesses, as follows: replay attack, and man-in-the-middle (MITM) attack. Thus, they proposed the robust dynamic user authentication scheme for WSNs [41]. Nonetheless, there proposition does not provide complete mutual authentication. An improved robust dynamic user authentication scheme is proposed in [42]. This scheme modified version of the robust scheme in [41]. It protects against replay attacks of login message, forgery attacks, MITM attacks and can provide mutual authentication between login node and GW node as well as mutual authentication between the GW node and the user.

In [51], Manik Lal Das also shows that Wong et al.'s scheme is vulnerable to many logged in users with the same login-id threat, that is,who has a valid user's password can login to the network. The protocol also suffers from stolen-verifier attack, because both the GW-node and login-node maintain the lookup table of registered users' credentials. He proposes a two-factor user authentication protocol for WSN which aims to devise a user authentication protocol that eliminates the weaknesses of Wong et al.'s protocol and provides strong authentication, session key establishment, and achieves efficiency. It resists many logged in users with the same login identity, stolen-verifier, guessing, impersonation and replay threats.

The basic idea of his scheme is that a user will receive a personalized smart card from the GW-node at the time of the

TABLE III
TOTAL COST OVERHEAD FOR SCHEMES.

Protocols	Total Cost Overhead
Wong et al.'s scheme [39]	$7T_H$+$4T_{XOR}$+$3C_{MH}$
Tseng et al.'s scheme[40]	$5T_H$+$4T_{XOR}$+$3C_{MH}$
Vaidyaet al.'s Robust scheme [41]	$8T_H$+$4T_{XOR}$+$3C_{MH}$
Vaidya et al.'s Improved Robust scheme[42]	$11T_H$+$4T_{XOR}$+$3C_{MH}$
L. Das al.'s Two-Factor UA scheme [51]	$12T_H$

T_H: the time for performing a one-way hash function *h()*.
T_{XOR} : the time for performing an XOR operation.
C_{MH} : the delay time for the communication taken place between the login-node and the GW-node in multi-hops.

registration process and then, with the help of user's password and smart card, the user can login to the GW-node and access data from the network.

Table III shows the overall cost of these schemes. The total cost overhead is the sum of computation and communication costs for all phases.

D. Comparison and analysis

The Table IV summarizes the comparison between all approaches. Although a direct comparison of all metrics might not be appropriate due to the different approaches used in each setting. We propose to the next, four metrics: the key mode witch be symmetric (Sym) or asymmetric (Asym), the scalability, and the communication complexity witch depend on node density. In communication complexity, *n* denote the number of sensor nodes in user's communication range, *N* the network size, O(1) means that, in the protocol, communication is not depend on node density, the T_{EXP} denote the time for performing a modular exponential computation. The last metric in the comparison is the topology witch can be flat or hierarchical (Hierar) .

TABLE IV
COMPARISON BETWEEN THE DIFFERENT APPROACHES.

Solutions	Key mode	Scala-bility	communication complexity	Topology
Vaidya et al.'s scheme[42]	Sym	Yes	$11T_H$+$4T_{XOR}$+ $3C_{MH}$ =O(1)	Hierar
Realizing Robuste User Authentication [17]	Asym	Yes	2nT_H+$3T_{EXP}$ =O(n)	flat
Symmetric Key Based Authenticated Querying [21]	Sym	No	O($\sqrt{N}$)	flat
Sinle Key Chain[53]	Sym	No	O(1)	flat
Merkle hash tree [53]	Sym	No	O(1)	flat
NACP[5]	Asym	Yes	$2T_{EM}$+$5T_H$=O(1)	flat

In some schemes such as [2], and the user's authentication schemes, we have two types of nodes: regular sensor node, and controller or login node witch are more powerful nodes and perform more operations than regular nodes. They can be used in hierarchical topology, where controller or login node is used as cluster head. In the others schemes, all sensors are regulars and perform the same operations. They can be used in homogeneous topology.

V. CONCLUSION

Many security solutions are based on Public Key Cryptography, highly expenses and vulnerable to Replay and DoS attacks. Most of access control protocols are based on key pre-distribution mechanisms, combined with or not a one way key chain or a pseudo-random function. In that's case, the access control solution includes all vulnerabilities of the mechanism which it is based and its security depends also on that it. Thus, it's a very challenge to integrate in one protocol, the access control scheme and key management scheme to optimize security solution for WSNs.

REFERENCES

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

[2] K. An Liu,R. Peng Ning, D. Maughan, Securing Network Access in Wireless Sensor Networks, WiSec'09, March 16 9,2009, Zurich, Switzerland. Copyright 2009 ACM 978-1- 60558-460-7/09/03

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

[4] Donggang Liu, Peng Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," in Proc. of ACM Conference on Computer and Communications Security (CCS), 2003

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

[6] H. Chan, A. Perrig, D. Song, Random key pre-distribution shemes for sensor networks, IEEE Symposium on Security and Privacy, 2003, pp. 197-213.

[7] S.J. Choi, H.Y. Youn, An efficient key pre-distribution scheme for secure distributed sensor network, The 2005 IFIP International Conference on Embedded and Ubiquitous Computing (EUC'2005), LNCS 3823, 2005, pp. 1088-1097.

[8] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, Proceedings of the 9th ACM Conference on Computer and Communication Security, 2002, pp. 41-47.

[9] C.W. Park, S.J. Choi, H.Y. Youn, A novel key pre- distribution scheme with LU matrix for secure wireless sensor networks, International Conference on Computational Intelligence and Security (CIS 2005), Springer-Verlag, Germany, 2005, pp. 494-499, LNAI. 3801, Part I, Dec.

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

[11] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM 21 (Feb. 1978) 120-126.

[12] Y. Zhang, W. Liu, W. Lou, Y. Fang, Location-based compromise-tolerant security mechanisms for wireless sensor networks, IEEE JSAC, Special Issue on Security in Wireless Ad Hoc Networks, vol. 24, no. 2, 2006, pp. 247-260.

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

[14] H. S. Kim and S. W. Lee, "Enhanced novel access control protocol over wireless sensor networks," IEEE Trans. Consum. Electron., vol. 55, no. 2, pp. 492- 498, 2009.

[15] H. Lee,K. Shin,D. Lee, Practical Access Control Protocol for Secure Sensor Networks, The 13th IEEE International Symposium on Consumer Electronics (ISCE2009)

[16] P. Zeng, K-K..R Choo, D. Sun, "On the Security of an Enhanced Novel Access Control Protocol for Wireless Sensor Networks", IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, May 2010, pages 566-569

[17] Z.Benenson, N. Gedicke and O. Raivio, Realizing Robust User Authentication in Sensor Networks, Workshop on Real-World Wireless Sensor Networks (REALWSN), Stockholm, Sweden,June 2005.

[18] G. Gaubatz, J.-P. Kaps, and B. Sunar. Public key cryptography in sensor networks - revisited. In ESAS, pages 2{18, 2004}.

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

[20] D. Liu and P. Ning. Establishing pairwise keys in distributedsensor networks. In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, pages 52{61. ACM Press, 2003}.

[21]] S. Banerjee,D. Mukhopadhyay, "Symmetric Key Based Authenticated Querying in Wireless Sensor Networks", InterSense '06, Proceedings of the First International Conference on Integrated Internet Ad hoc and Sensor Networks, May 2006, Nice France.

[22] C. Blundo et al. "Perfectly-secure key distribution for dynamic conferences", in Advances in Cryptology CRYPTO 92, LNCS, 1993, pp. 471-486.

[23] S. Dulman, P. Havinga and J. Jurink, Wave leader election protocol for wireless sensor networks, MMSA Workshop, Delft, The Netherlands, December 2002.

[24] Z. Benenson, L. Pimenidis, F. C. Freiling, and S. Lucks. Authenticated query ooding in sensor networks. In PERCOMW '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Com-puting and Communications Workshops, page 644, Washington, DC,USA, 2006. IEEE Computer Society.

[25] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas. Multicast security: A taxonomy and some efficient constructions. In Proc. IEEE INFOCOM'99, volume 2, pages 708-716, New York, NY, Mar. 1999. IEEE.

[26] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security, pages 41-47. ACM Press, 2002.

[27] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong. The design of an acquisitional query processor for sensor networks. In SIGMOD '03: Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data,pages 491-502, New York, NY, USA, 2003. ACM Press.

[28] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. SPINS: security protocols for sensor networks. Wireless Networks, 8(5):521-534, 2002.

[29] S. Ganeriwal, S. Capkun, C.-C. Han, and M. B. Srivastava. Secure time synchronization service for sensor networks. In WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, pages 97-106, New York, NY, USA 2005. ACM Press.

[30] S. Seys and B. Preneel. Efficient cooperative ignatures: A novel authentication scheme for sensor networks. In 2nd International Conference on Security in Pervasive Computing, number 3450 in LNCS, pages 86 - 100, April 2005.

[31] A. K. Awasthi, and S. Lal, "A remote user authentication scheme usingsmart cards with Forward Secrecy," IEEE Transactions on Consumer Electronics, vol.49, no.4, p.1246-1248, Nov. 2003.

[32] M. S. Hwang, C. C. Chang, and K. F. Hwang, "An 1Gamal-like cryptosystem for enciphering large messages," IEEE Trans .on Knowledge and Data Engineering, vol.14, no.2, pp.445-446, 2002.

[33] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," ACM Operating Systems Review, vol.36, no.4, pp.23-29, 2002.

[34] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," IEEE Trans. on Consumer Electron., vol.49, no.2, pp.414- 416, May 2003.

[35] H. M. Sun, "An Efficient remote user authentication scheme using smart cards," IEEE Trans. on Consumer Electron., vol. 46, no. 4, pp. 958-961, Nov. 2000.

[36] B. Schneier, "Applied Cryptography," John Wiley & Sons Inc., 1996.

[37] M. Lal Das,A. Saxena,V. Gulati, A Dynamic ID-based Remote User Authentication Scheme, IEEE Transactions on Consumer 630 Electronics, Vol. 50, No. 2, MAY 2004

[38] C.Y. Lee, C.H. Lin, and C.C. Chang, "An Improved Low Communication Cost User Authentication Scheme for Mobile Communication", Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications (AINA 2005), Taiwan, March 2005.

[39] Wong, K. H. M., Zheng, Y., Cao J., and Wang, S. 2006. A dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06) Jun. 2006; 1: 318- 327.

[40] Tseng, H. R., Jan, R. H., and Yang, W. 2007. An improved dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE Global Communications Conference (GLOBECOM'07), Nov. 2007;986-990.

[41] B. Vaidya,J. S Silva,J. Rodrigues, Robust Dynamic User Authentication Scheme for Wireless Sensor Networks, Q2SWinet'09, October 28-29, 2009, Tenerife, Canary Islands, Spain.

[42] Binod Vaidya, Min Chen2 and Joel J. P. C. ,Rodrigues3, Improved Robust User Authentication Scheme for Wireless Sensor Networks Improved Robust User Authentication Scheme for Wireless Sensor Networks December 2009

[43] D. Naor, M. Naor and J. Lotspiech "Revocation and Tracing Schemes for Stateless Receivers", CRYPTO '2001 44] R. Merkle. Protocols for public key cryptosystems. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Apr 1980.

[44] Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proceedings of the 2003 IEEE Symposium on Security and Privacy, pp. 197-213 (May 2003)

[45] Lai, B., Kim, S., Verbauwhede, I.: Scalable session key construction protocol for wireless sensor networks. In: Proceedings of the IEEE Workshop on Large Scale RealTime and Embedded Systems LARTES (December 2002)

[46] Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM conference on Computer and commu- nications security, pp. 41-47 (November 2002)

[47] Anderson, R., Chan, H., Perrig, A.: Key Infection : Smart Trust for Smart Dust. In: Proceedings of the 12th IEEE International Conference on Network Protocols, pp. 206-215 (October 2004)

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

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

[50] C. Castelluccia, E. Mykletun, and G. Tsudik. Efficient aggregation of envrypted data in wireless sensor networks. In MOBIQUITOD'05: Proceedings of The Second Annual Internationnal Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005

[51] M. L. Das,Two-Factor User Authentication in Wireless Sensor Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 3, MARCH 2009

[52] J. Wu,S. Shimamoto, Usage Control based Security Access Scheme for Wireless Sensor Networks. IN IEEE ICC 2010 proceedings

[53] SHEN Yu-long , MA Jian-feng , PEI Qing-qi: An Access Control Scheme in Wireless Sensor Networks. In: Proceedings of 2007 IFIP International Conference on Network and Parallel Computing - Workshops, pp. 362-367