DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4607

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURE AND AUTHENTICATED KEY ESTABLISHMENT SCHEME FOR WIRELESS SENSOR NETWORK

U. Mekala
Research Scholar
Department of Computer Science
Bharathidasan University
Trichy-23, Tamilnadu, India
:

K. Muthuramalingam
Assistant Professor
Department of Computer Science
Bharathidasan University
Trichy-23, Tamilnadu, India

Abstract: Information security in frame less wireless sensor networks (WSNs) is one of the most significant research challenges. Encryption and key distribution are significant primitives to build secure Wireless Sensor Networks (WSN). A large amount of dissimilar key distribution schemes were implemented, targeting different types of WSNs. In these networks, sensor nodes are typically speckled liberally in the field in order to monitor, gather, disseminate, and deliver the sensed data to the control node. Various studies have listening carefully on key establishment schemes in homogeneous WSNs. However, recent investigation has shown that achieving survivability in WSNs requires a hierarchy and heterogeneous substructure. In this research, to address security issues in the assorted WSNs, propose a secure clustering scheme called Attribute based Encryption (ABE) along with a deterministic pair-wise key administration scheme based on public key cryptography and attribute based encryption algorithm. The proposed security device guarantee that any two sensor nodes positioned in the same cluster and routing path can directly establish a pair-wise key without disclosing any material to other nodes. Through safekeeping performance evaluation, it is shown that the proposed scheme guarantee node-to-node validation, high resiliency against node capture, and minimum remembrance space requirement.

Keywords: Key Establishment Scheme, Wireless Sensor Network, Attribute based Encryption, Elliptic Curve Cryptography, Node-to-node Authentication, Key Distribution.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have changed most appealing analysis area, because it is a useful inherent characteristic such as small capacity, scalability of nodes, and easy to use. Large scale of WSNs is envisioned to be widely applied in various submissions such as object tracking, environment checking and data gathering in the near future. Typically, a WSN is self-possessed of a large number of sensor nodes; each sensor node is a small, inexpensive wireless device with limited battery-operated power, memory storage, data dispensation capacity and short radio transmission range.

The main appearances of WSN include: wireless nature of announcement, resource limitation on sensor nodes, lack of fixed infrastructure, unknown network topology prior to deployment, and high risk of physical attacks on unattended sensors. In order to design a practical WSN, many deliberations should be taken into the account. Security is one of the most important subjects, since it is going to be deployed in unattended atmosphere. Depending on applications used for WSNs, security is the principal challenge in WSNs and security aspect is indispensable for WSNs before scheming WSNs [1].

The energy-constrained nature of the sensor systems makes the task of integrating security as challenging problem. [2] Argued that, most of the well-known security instruments introduce significant upstairs and require a lot of computation and announcement resource.

Generally security protocols would provide the WSN with three capabilities: encryption, confirmation, and key management. Key organization is the process by which cryptographic keys are generated, stored, threatened, transferred, loaded, used, and demolished. It is critical to meet the safekeeping goals of confidentiality, integrity and substantiation to prevent the nodes being negotiated by an adversary. Accordingly, key management is a crucial part of security in WSN and has been densely investigated recently.

For WSN, key management protocols can be confidential into four categories: symmetric key protocols, asymmetric key protocols, trusted third party protocols, and key pre-distribution conventions [3]. If an attacker compromises one node and extracts, it is master key. All nodes and the exchange messages among them will be co-operated. Trusted third party protocol is suffering from both lack of scalability and single point disappointment. Because the communication entities can achieve mutual confirmation and secure communication through the single confidential third party's assistance. Finally, adopting pre-distribution where the required secret keys are pre-loaded before positioning the nodes has many limitations: it has no immunity in contradiction of node's capture attack, and it does not enhance the flexibility and scalability of the WSN.

II. RELATED WORK

In delivering common communications to a certain group of devices, it is more operative to send multicast communications rather than unicast messages. Multicast announcement is recommended for embarrassed IoT networks to reduce the bandwidth usage, and minimize the energy ingesting and processing overhead at the terminals [1]. Establishing a group key among the appropriate members, would enable the secure and trustworthy delivery of messages within a multicast group. Although Datagram Transport Layer Security (DTLS) greeting is designed for device-to-device substantiation [6] in IoT, it does not support multicast security [1].

Security and key management in WSNs is a widely deliberated topic [7] [9]. The WSN group key executive protocols such as MIKEY [10] and TESLA [11] are at a halt not there compatibility with IoT individuality, For instance, the MIKEY architecture is entirely designed to facilitate multimedia distributions, whereas TESLA is proposed for the broadcast authentication of the source and not for protecting the confidentiality of multicast messages. Likewise, the Topological Key Hierarchy (TKH) lowers the communication cost of rekeying messages by generating a key-tree based on the underlying topology of WSNs [12]. However, in TKH, the calculation and communication costs grow linearly with the number of collection members. Secret sharing is used for different security protocols of WSNs including key management and data concealment [4], [13], [14].

The authentic group key transfer protocol proposed in [4] requires an on-line key generation center (KGC) to construct and allocate the group key, which increases the overhead to contrivance the system, and reduces flexibility. This work has paved the way to reproduce the inputting scheme in [13], which is more dynamic without a trusted KGC. The group key initiator is amongst the group memberships and all the members equally participate in the final key derivation. However, both schemes [4] and [13] contain pairing-based calculations, which do not provide inescapable cipher suites for globally connected IoT devices.

III. THE PROPOSED PROTOCOL FOR AUTHENTICATED WIRELESS SENSOR NETWORKS AND KEY MANAGEMENT

This protocol is based on a amalgamation of three different techniques. These performances are asymmetric encryption, trusted third party, and pre-distribution. The proposed protocol for authenticated wireless sensor networks and key management is adopting the unbalanced cryptographic scheme to generate sovereign session keys. These scheme assurances that two collaborating parties can establish a unique session key between them.

Furthermore, it is using key pre-distribution apparatus for a large-scale WSN, based on a hierarchical clustered system model and trusted third party. Comparing with existing protocols, this integrated protocol can provide sufficient security no matter how many sensors are cooperated, fixed key storage above, full network connectivity, and low communication above can also be achieved. Consequently, it enhances the immunity against different types of attacks. Moreover, this protocol offers a high level of security for WSN with seeing it is limited recourses. So it creates a balance between both security and controlled resources, by combining different security techniques and making use of their advantages and incapacitating their boundaries. WSN is assumed to be composed of a number of dispersed head clusters with heads.

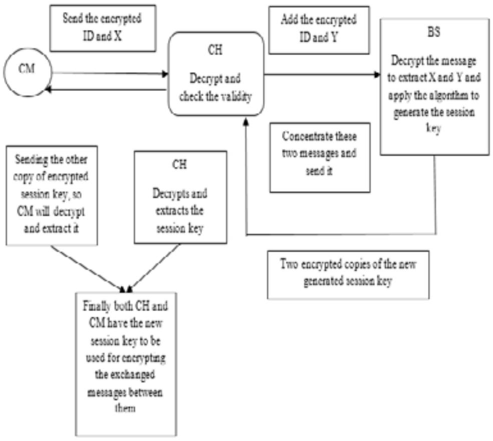
Send the encrypted ID and X
CM
CH
Decrypt and check the validity
Add the encrypted ID and Y
BS
Decrypt the message to extract X and Y and apply the algorithm to generate the session key
Concentrate these two messages and send it
Sending the other copy of encrypted session key, so CM will decrypt and extract it
CH
Decrypts and extracts the session key
Two encrypted copies of the new generated session key
Finally both CH and CM have the new session key to be used for encrypting the exchanged messages between them

Figure 1: Key Generation Process

The base location or the trust intermediary will be responsible about both organizing the nodes into clusters and influential the cluster head for each one. Furthermore, the base redistribution will pertain an election algorithm, to allow a cluster head to take over instead of another offended one to avoid single point failure. Actually, this protocol does not use node to node communication. Nodes can communicate only with their cluster heads. Therefore, each node needs only one hop to reach its closest cluster head. Thus decreases the network traffic and enhances the scalability. The protocols take benefit of asymmetric cryptographic to solve the pre-distribution restrictions. Each node of WSN will be pre-loaded with two keys (Private and Public). In this case the number of stored keys at each node is preset, and it will not be enlarged with the augmented number of nodes. So each node has to store only its cluster head's public key, instead of storing the number of public keys equals the number of organized nodes. This will save the storage capacity for each node and preserve the scalability of WSN. Furthermore, these deposited keys will be used to generate a new session key, so for each new link a new meeting key will be generated. If an attacker could cooperation a node the other nodes will not be affected, since each one of them has a dissimilar session key.

A. Attribute based Encryption:

Attribute-based encryption (ABE) is a moderately recent approach that reassesses the concept of public key cryptography. In obsolete public-key cryptography, a message is encrypted for a precise receiver using the receiver's public-key. Identity-based cryptography and in exacting identity-based encryption (IBE) altered the traditional understanding of public-key cryptography by allowing the public-key to be an uninformed string, e.g., the email report of the receiver.

ABE spirits one step additional and defines the identity not atomic but as a set of attributes, e.g., roles, and communications can be encrypted with respect to subsets of characteristics (key-policy ABE - KP- ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE). The key issue is that someone should only be able to decrypt a ciphertext if the individual holds.

a. Setup (d):

The authority consistently and arbitrarily chooses t1, ..., tn, y from Zq, and distributes the public key, PK =(T1 = g t1 , ..., Tn = g tn , Y = e(g, g) y). And the master key is MK = (t1... tn, y).

b. KeyGen (AU, PK, MK):

The authority executes and produces a private key for the data user U. Choose a d− 1 degree polynomial q haphazardly such that q (0) = y. The data user’s private key D is {Di = g q (i) ti} ∀i∈AU.

c. Encrypt (ACT, PK, and M):

Data owner encodes message M ∈ G2 with a set of characteristics ACT. Choose a random number s ∈ Zq, and the translated data is available as CT = (ACT, E = MY s = e (g, g) ys, {Ei = g tis} ∀i∈AU).

d. Decrypt (CT, PK, D):

Data user decrypts the translated data CT with the private key D. Choose d attributes from i∈ AU T ACT to calculate e(Ei , Di) = e(g, g) q(i)s if |AU T ACT ≱ d. And compute Y s = e (g, g) q (0) s = e (g, g) ys with the Lagrange coefficient, and the communication M = E/Y s can be attained.

B. Elliptic Curve Cryptography:

Elliptic Curve Cryptography (ECC) is a public key cryptography. Where each user or the expedient taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the certain user knows the private key whereas the public key is distributed to all users enchanting part in the communication. Public-Key cryptography (PKC) systems can be used to provide secure infrastructures over insecure frequencies without exchanging a secret key.

The most popular public-key cryptography systems today are RSA and Elliptic Curve Cryptography (ECC). Due to directness of wireless sensor networks, secure announcement between nodes is necessary. The Elliptic Curve Cryptography (ECC)] is based on algebraic concepts related with elliptic curves over limited fields Fp or F2m. Elliptic Curve encryption and decryption system necessitates appoint G and an elliptic group E_q (a, b)as a parameters.

a. **Encryption using ECC**

To encrypt and send a message Pm to B, A chooses a random positive integer k and produces the cipher text Cm as given by equation consisting of the pair of points.

$$Cm = [k*G, Pm +k*P_B] \qquad (1)$$

Here A has used B's public key P_B.

b. Decryption using ECC

To decrypt the cipher text, B multiples the first point in the pair by B's private key nB and subtracts the result from the second point as shown by equation.

$$Pm+ k *P_B - n_B (k*G) = Pm+ k (n_B* G) - n_B (k*G) =Pm \qquad (1)$$

A key exchange between users A and B can be explained as following steps:-

- A select an integer n_A< n as A"s private key.
- A generates a public key P_A = n_A*G which is a point in
- E_q (a, b).
- B select an integer n_B< n as B"s private key.
- B generates a public key PB= nB*G which is a point in E_q(a, b).

.Public keys are exchanged between A and B. A generates the secret key K= nA* PB and B generates the secret key K= n_B* P_A

C. Security in Network:

This section characterizes a comprehensive evaluation of the projected protocol, by discussing three main aspects. Firstly, the contributions that the projected protocol is added, by taking the beneficial of combining three different mechanisms for authentication and key organization. It makes use of the strong point of these mechanisms and overpowers their boundaries. Secondly, evaluating the performance of the projected protocol based on specific norms which are used to compare the proposed security procedures for WSN. Mainly, the performance of this protocol reflects on the efficient energy ingesting.

Thirdly, the security which is measured as the most important concern in this field. The proposed procedure provides a high level of security, since it is meeting the fundamental requirements of a secure WSN, and promising the immunity against different security attacks. Moreover, it provisions three security services: encryption, authentication, and key management. Computation overhead: In WSNs scenario, it is highly desirable for a security protocol to have low computational overhead on resource embarrassed sensor nodes. Many specialists argued that using disproportionate cryptographic as an authentication mechanism in WSN is not practical. Because of it is related encryption algorithms have expensive calculations, so it is not well-matched with the limited possessions of WSN.

Table I: Simulation Setup

Simulation setup	Value	ABE	ECC
Number of Nodes (Complete Transaction)	50	45	40
Distribution of Nodes	Random with Mobility	Random with Mobility	Random with Mobility
Mobility Model	Random Waypoint	Random Waypoint	Random Waypoint
Operational Mode	802.11		
Data Rate	11 Mbps	10 Mbps	9 Mbps
Simulation time	3600 seconds	3200 seconds	3400 seconds

IV. RESULT AND DISCUSSION

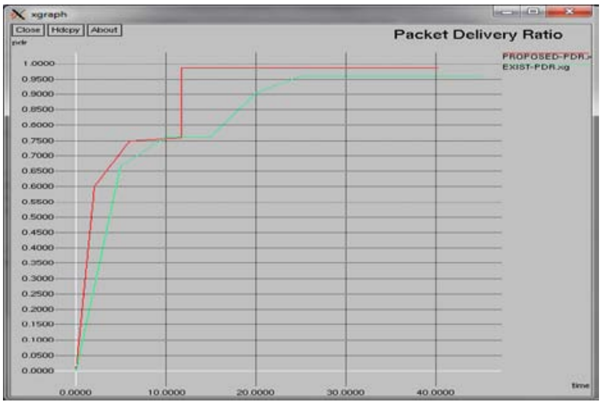

Figure 2: Security Analysis

Packet-delivery ratio- Fig.4.1 describes the packet delivery ratio comparison between existing and proposed system. It is amount of packets actually delivered at the sink. In the simulation of algorithm, the subsequent results are obtain these are the simulation outcome of algorithm, Attribute based Encryption (Symmetric) and Elliptic Curve Cryptography (Asymmetric). The proposed algorithm for symmetric and asymmetric algorithms provide the better results from the aspects of security

In an outer layer, simulation results prove the viability of the projected distributed approaches in the studied context of IoT keying, which includes highly resource-constrained swellings sensor platform. Providing almost equivalent energy costs associated to the simple distributed approach, the threshold dispersed approach introduces supplementary recovery and secrecy possessions, both essential for a collaborative protocol.

The Finished message ends the handshake conversation. It includes a hash computed over the master key and all the past communications. The receiving entity is able to compute the conforming hash value from its own records in order to check if the result matches the received value. These results were expected since assigning the computation of DH modular exponentiations (in the key agreement mode) leads to more energy savings at the measured device than off loading signature and encryption operations in the key transport mode.

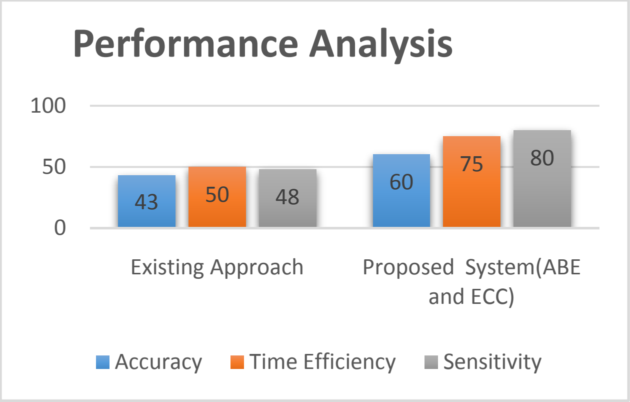

Figure 3: Performance Analysis between Existing and Proposed Approach

Energy savings can be augmented by reducing the duration of listening mode. Using LPL (Low Power Listening) protocols, the source node can be temporarily put into a sleep mode when waiting for the procedure to run between proxies and server. These saving can be especially important for the key arrangement protocols, where the listening announcement cost amounts to more than 50% of the overall energy ingesting. The results also show that the energy costs of the threshold dispersed approach in the key agreement mode of IKE are slightly less small than those of the simple disseminated approach; contrary to what may have been expected if one had only measured the additional cost of the compeers of the polynomial shares.

V. CONCLUSION

It is clear that the possible of the wireless sensor networks (WSN) paradigm will be fully unchecked once it is connected to the Internet, becoming part of the Internet of Things (IoT). In this research, a new three party key establishment scheme for Internet-enabled measuring device systems as part of Internet-of-Things was proposed. By presented our key formation scheme based on traditional Internet style key establishment and long term master-individual keys as a DoS unaffected version of two well-known previous arrangements. In comparison to the previous well-known three-party arrangements, our extension not only injections DoS susceptibility, but also provides some other advantages such as important efficiency. The proposed key establishment scheme can be used not only for founding shared key between any two sensors, but it is applicable for founding shared secret amongst any two entities/ things in the background of IoT.

VI. REFERENCES

[1] S. Keoh, S. Kumar, O. Garcia-Morchon, E. Dijk, and A. Rahman. (Feb. 2014). DTLS-Based Multicast Security for Low-Power and Lossy Networks (LLNs). [Online]. Available: http://tools.ietf.org/pdf/draft-keohdice-multicast-security-05.

[2] J. Zhang and V. Varadharajan, ``Wireless sensor network key management survey and taxonomy," J. Netw. Comput. Appl., vol. 33, no. 2, pp. 6375,2010.

[3] Rahman and E. Dijk. (Oct. 2014). Group Communication for the Constrained Application Protocol (CoAP). [Online]. Available: https://tools.ietf.org/html/rfc7390

[4] L. Harn and C. Lin, ``Authenticated group key transfer protocol based on secret sharing," IEEE Trans. Comput., vol. 59, no. 6, pp. 842846, Jun. 2010.

[5] W. Yuan, L. Hu, H. Li, and J. Chu, ``Security and improvement of an authenticated group key transfer protocol based on secret sharing," Appl. Math. Inf. Sci., vol. 7, no. 5, pp. 19431949, 2013.

[6] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, ``DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Netw., vol. 11, no. 8, pp. 27102723, 2013.

[7] P. Nie, J. Vähä-Herttua, T. Aura, and A. Gurtov, ``Performance analysis of HIP diet exchange for WSN security establishment," in Proc. 7th ACM Symp. QoSSecur. Wireless Mobile Netw., 2011, pp. 5156.

[8] P. Porambage, P. Kumar, C. Schmitt, A. Gurtov, and M. Ylianttila, ``Certificate-based pairwise key establishment protocol for wireless sensor networks," in Proc. IEEE 16th Int. Conf. Comput. Sci. Eng. (CSE), Dec. 2013, pp. 667674.

[9] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, ``Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2014, pp. 27282733.

[10] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman. (Aug. 2004). MIKEY: Multimedia Internet

Keying. [Online]. Available: http://www.rfc-base.org/txt/rfc-3830.txt

[11] Perrig, D. Song, R. Canetti, J. D. Tygar, and B. Briscoe. (Jun. 2005).Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multi- cast Source Authentication Transform Introduction. [Online]. Available: http://www.ietf.org/rfc/rfc4082.txt

[12] J.-H. Son, J.-S. Lee, and S.-W. Seo, ``Topological key hierarchy for energyefficient group key management in wireless sensor networks," Wireless Pers. Commun., vol. 52, no. 2, pp. 359382, 2010.

[13] C.-Y. Lee, Z.-H. Wang, L. Harn, and C.-C. Chang, ``Secure key transfer protocol based on secret sharing for group communications," IEICE Trans. Inf. Syst., vol. 94, no. 11, pp. 20692076, 2011.

[14] R. Di Pietro and S. Guarino, ``Data confidentiality and availability via secret sharing and node mobility in UWSN," in Proc. IEEE INFOCOM, Apr. 2013, pp. 205209.

[15] Certicom Research, Standards for Efficient Cryptography. (Sep. 2000). SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0. [Online]. Available: http://www.secg.org/SEC2-Ver-1.0.pdf