Light Weight Two-level Session Key Management for End User Authentication in Internet of Things

Zahid Mahmood, Huansheng Ning*
School of Computer and Communication Engineering,
University of Science and Technology Beijing,
Beijing 100083, China.
zmakash5@yahoo.com, ninghuansheng@ustb.edu.cn

AtaUllah Ghafoor
Department of Computer Science,
National University of Modern Languages,
Islamabad 44000, Pakistan.
ataullah@numl.edu.pk

***Abstract*—Central entity attains process and provides authentication for Wireless Sensor Network (WSN) architecture. On the other hand, Internet of Things (IoT) sensors sense data, make collaboration, acquired information and provide to end users who act like a distributed architecture. Secure yet lightweight protocol for communication over the Internet is a pertinent problem in constrained environments in the context of Internet of Things (IoT) / HMA Chain to HMA Chain (M2M) applications. Proper authentication and reliable transmission of secure data at end-to-end communication link are important in IoT. This paper contributes a Two Level Session Key (TKS) based authentication mechanism for IOT scenario. The proposed TKS authentication and secure communication procedure permit sensor nodes and the end-users to authenticate each other and initiate secure connections in IoT-based architecture. The proposed protocol supports the resource insufficiency edge nodes, heterogeneity, and scalability of the network. The presentation and security investigation give a good reason that the proposed scheme is feasible to set up in a resource constrained environment. To integrate communication authors used Message Authentication Code (HMAC) during node association phase, which resists for replay and DOS attacks. Key size, energy consumption, memory overhead, and foolproof communication are the main concern for constrained devices. TKS provided lightweight and secure communication between end-to-end users without any third-party authentication sources, after authenticating and establishing one level session key**

Keywords— Distributed Internet of Things, Wireless Sensor Networks, authentication, secure communication.

I. INTRODUCTION

Recent advances in wireless communications and pervasive computing are driving the constant development of the theoretical Internet of Things (IoT). Inter of Things (IoT) involves the everyday useable entities in our surroundings that can become proactive nodes of Internet, cellular and WSN in future. Data collection from different nodes in different networks is a challenging task. It needs a uniform information format for the end user in IoT paradigm. Industry and academia jointly investigated the WSN and its security challenges during the last decade. Although the existing data security techniques, concepts and application have no novelty for IoT and security is still challenge. Nevertheless, an extensive amount of research work has been done to spot out the confronts and possible security mechanisms for securing IoT as shown throughout references [1], [2], [3], [4], and [5].In the framework of IoT appliance area, WSN architectures exist as centralized and distributed approaches [6]. In centralized networks, there is little or no support to access the data sensing network devices directly. The distributed networks allow the end-users and other network entities to obtain raw data straight away from the sensor nodes. Even though provisioning of services is located at the edge of the network, different application platforms and end-users can collaborate energetically with each other. As a result of the decentralized and distributed nature of the network, it is necessary to judge the sheltered organization of identity and authentication of connecting nodes. Cryptographic key management is a fundamental block in the network security. In small devices, due to their resource constrained nature, the symmetric key pre-distribution techniques were considered more suitable. With the advent of Elliptic curve cryptography (ECC), many researchers explored the applicability of asymmetric key Taking further work on elliptic curve key exchange mechanism. Identity-based key management makes use of bilinear pairing on elliptic curves. Even though identity-based key management techniques provide features like self-authentication, online key calculation, key update mechanisms, and scalability but, still bilinear pairing function is used during the key calculation, and the same, its uses more computational resources. This paper proposes a hybrid key management technique where identity-based key management is applied to establish secure connectivity among the nodes of the hierarchy nodes like connecting a hub, cluster heads (CHs) and a base station (BS). A pairwise probabilistic key predistribution scheme is applied to secure the internodes communication. It involves two levels for establishing session key to strengthening the key against traffic analysis attacks.

The remainder of this paper is structured as follows. Section II reviews recent proposals addressing different security aspects on IoT scenarios. Section III provide detail scenario of two-way session key establishment and background for the proposed scheme. Analysis, performance, and results of proposed scheme present in section IV. Section V concludes the paper and provides a direction for future work

II. RELATED WORK

We have explored different related schemes to identify that some

IoT applications may be more efficient to use a peripheral device to manage cryptographic functions and store security keys. Authentication-oriented peripherals can also be used on wearable IoT devices that require consumable sensors, such as sensor strips or pads. The low-cost peripheral can be embedded in the consumable and will guarantee the consumable is a reliable source, works with the measurement device and has not been used more than allowed. Network security relies on symmetric key cryptography (SKC), message authentication code and public key cryptography to provide confidentiality, integrity, and authentication. SKC uses the same key to encrypt and decrypt the data. Encryption assures confidentiality of data, where it is transmitted through the wireless link. To support integrity requirement of the received data, message authentication codes (HMAC) are used. However, before encryption, the data using SKC algorithm, all the parties involved in communication should agree upon a secret key. For this purpose, key exchange mechanism based on asymmetric cryptographic primitives can be used. In asymmetric or public key cryptography (PKC), the recipients' public key is used for encryption, while decryption is done by recipient's private key. Camtepe at El [7] gives a detailed classification of symmetric key distribution protocols for two different scenarios: distributed and hierarchical WSNs. In each scenario, the authors analyze diverse mechanisms to establish pair-wise and group-wise keys between sensor nodes. Thus, Wang et al. [8] propose a grouping of symmetric key administration conventions in WSN, yet taking into account the system structure and the likelihood of key sharing between a couple of sensor hubs. Their works at a first level separate concentrated and appropriated key plans. At a second level, they give other separation given the probabilistic and deterministic key foundation systems. Roman et al. [9] give an abnormal state grouping taking into account the key administration frameworks (KMS), in particular: key pool structure, a scientific system, arrangement system and open key structure. They reason that open key cryptography can be a suitable answer for sensor hubs that keep running as customer hubs (in the model client–server). For server hubs, numerical based KMS, for example, polynomial plan, give better exhibitions. The previously mentioned approaches don't adequately cover conceivable key appropriation instruments (deviated and symmetric techniques), for instance, just symmetric methodologies are contemplated in [7,8]. Plus, they give heterogeneous arrangements because of diverse disconnected criteria, as in [8, 9]. L.Eschenauer at al [10] examined that in numerous situations, the edge hubs having a place with the same geological territory (e.g., healing center environment) are allowed personalities by a neighborhood character supplier (e.g., a focal server) for their confirmation and ID. Notwithstanding, the neighborhood substances do not just have the capacity to confirm to each other inside the gathering. Additionally, they have to speak with outside elements. In this manner, both the inner and outer substances need to recover impermanent personalities from a typical power, which empower them to validate each other and convey them to a typical platform Yosra [11], propose a few approaches to order key foundation approaches, for occasion in view of the utilized confirmation technique or the basic cryptographic primitive. As per Gartner's figure [12], the IoT, which rejects PCs, PDAs and tablets, will develop to more than 26 billion units introduced in 2020. Permitting every single physical article to interface with the Internet and to share data, may make more dangers than any other time in recent memory for our information and business mystery data. Concerned articles cover our ordinary cordial gadgets, for example, indoor regulators, refrigerators, stoves, clothes washers, and TV sets. It is anything but difficult to envision how terrible it would be if these gadgets were keeping an eye on us and uncovering our data. Nguyen at el. [13] depicted that the IoT offers a network for both human-to-HMA Chain and HMA Chain-to-HMA Chain correspondences. Sooner rather than later, everything is prone to be outfitted with little-implanted gadgets which can associate with the Internet. Such capacity is valuable for different spaces in our day by day life: i.e. from building mechanization, shrewd city, and reconnaissance framework to all wearable savvy gadgets. Be that as it may, the more the IoT gadgets are sent, the more noteworthy our data framework is in danger. Surely, a non-irrelevant number of gadgets in IoT are helpless against security assaults, for instance, foreswearing of administration and replay assaults, because of their obliged assets and the absence of insurance strategies. This sort of assaults prompts sensor battery consumption and results in poor exhibitions of detecting applications. Nguyen at El [14] expressed that creates the impression that an exceptional and all around characterized arrangement ready to ensure privacy in an IoT connection is as yet lost, as additionally attested in. I. Akyildiz and G.Sharmam at al [15 –16] give the value to note that numerous endeavors have been led in the WSN field yet a few inquiries emerge: Are the WSN proposition versatile to the IoT environment, considering both the heterogeneity of the included gadgets and the diverse application connections? How to handle the distinctive keys? Which sort of key dispersion instrument is the most reasonable? How to guarantee a conclusion to end trustworthiness confirmation component keeping in mind the end goal to make the framework stronger to noxious assaults? It empowers a remote client to safely arrange a session key with a sensor hub, utilizing an incline key understanding convention. J.-Y. Lee at el [17] guarantees common verification among clients, sensor hubs, and g portal hubs (GWN), in spite of the fact that the client never reaches GWN. With a specific end goal to apply such a plan to asset compelled models, it just uses basic hash and XOR calculations, as in M. Turkanovi [18] utilizing lightweight encryption technique given XOR control for hostile to duplicating and security assurance, so as to adapt to obliged IoT gadgets. Beginning from WSN connection, a client confirmation and key assertion plan for heterogeneous remote sensor systems is likewise proposed in. N. Ye at al [19]. The verification and access control technique displayed in goes for setting up the session key on the premise of Elliptic Curve Cryptography (ECC), another lightweight encryption system. This plan characterizes characteristic based access control approaches, oversaw by a trait power, upgrading shared confirmation among the client and the sensor hubs, and illuminating the asset compelled issue at the application level in IoT. Recently, Debiao He et al. [20] proposed a transient accreditation based shared confirmation and key assertion (MAAKA) plan for WSNs. In their plan, GWN issues a transient certification to every client and sensor hub with the assistance of secret key based validation. Utilizing the worldly accreditations, the client, the sensor hub and the GWN can verify each other. In their MAAKA plan, just hash capacity, and XOR operations are required. Subsequently, their plan is extremely proficient.

III. EFFICIENT KEY-MANAGEMENT SCHEME

In this section, we present our lightweight end-to-end key management protocol know as Two Level Session Key (TKS). Firstly, we present the system model and a set of assumptions and notations. In the light of above analysis presented in section-II, we found that to achieve confidentially and secrecy it is necessary

that secure key establishment using the third party is more secure. But on the other hand after authentication of IoT devices by the third party to achieve more secure communication two level sessions key plays an important role in hiding data and future communication between end user with revealing by the third party. In proposed scheme, connecting hub/Base Station (BS) issues a temporal credential to each user and sensor node with the help of password-based authentication. Using the temporal credentials, the user, the sensor node and the BS can authenticate each other. After completion of authentication process with the help of connecting a hub, Edge node and en-user establish secure session key know as a level-1 session key. After authentication, using level-1 session key both end exchange secret credentials with some nonce number and time stamp for generating Two Level Session Key (TKS) for future communication to resist against replay attack and data leakage in case compromising one authentication node. In their TKS scheme, only hash function, HMAC, and XOR operations are needed. Therefore, their scheme is very efficient. Detail scheme and its system model discuss in the following section. A list of notations is presented in Table 1.

Table-1: Notations for TKS

Notation	Description
N_S, N_C, N_P, N_W	Sensor Node, Cell Phone, Computer/Laptop, Wearable Device
T_{SN_C}	Time Stamp from N_C
V_{nN_C}	Nonce Value from N_C
D_{hN_C}	Hash of Data Set from N_C
R_{tsN_C}	Random number from N_C based on T_{stamp}
CH	Cluster Head
S_{nk}	Sink Node in WSN
BS	Base Station in Cellular Network
SVR	Server at LAN/WAN
$ID_{N_S}, ID_{N_C}, ID_{N_P}, ID_{N_W}$	Identity of Sensor Node, Cell Phone, Computer/Laptop, Wearable Device
$K_{N_s-N_C}$	Symmetric Key between N_S and N_C
SK_{REQ}	Session Key Request
$REG_{REQ\ CAT}$	Registration Request + Category of Request
$SK_{N_C-N_S}$	Session Key between N_S and N_C

A. System Model

We consider in proposed network system four main components; mobile and LAN user, base station, Sink Node, CH and sensor nodes. According to R. Roman [21], the main concept behind IoT is the pervasive presence around us of various wireless technologies such as Radio Frequency Identification(RFID) tags, sensors, actuators or mobile phones in which computing and communication systems are seamlessly embedded. L. Eschenauer [22] based on unique addressing schemes; these objects interact with each other and cooperate to reach common goals. Many small nodes are scatted randomly in the field to sense and communicate the data with the Base Station (BS), where the monitoring is carried out. The BS is a computationally powerful device, which monitors and control the flow of data within the network. Furthermore, the BS can be connected to the Internet to respond to the queries of remote users. From the security point of view, sensor nodes are openly deployed in the field and vulnerable to node capture attacks, the BS, located at a secure place and is connected to a more strong node know as sink node with the secure channel.

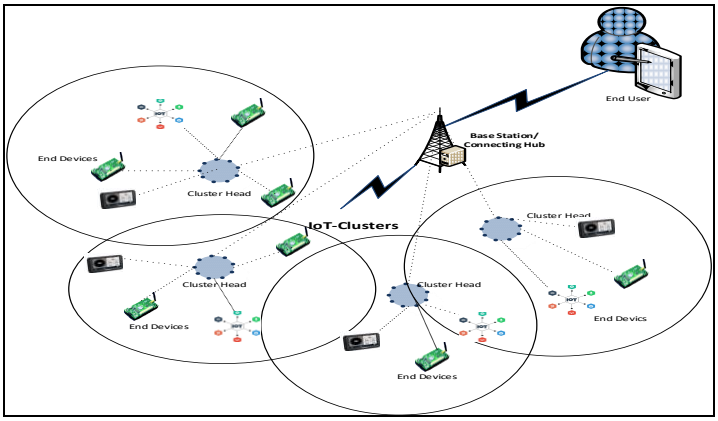

Figure-1 WSN Based IOT Architecture End to End Communication

In figure-1, we illustrate the assumed network architecture for proposed authentication scheme, where end-user can collaborate with different edge device to obtain the particular information or services. The edge network consists of heterogeneous devices and end user can be human or mobile. Based on fugure-1 authentication is considered for three communication scenarios particularly. (i) Mobile user asks for the request to get data from the particular sensor. (ii) Base station forwards this request to specific domain head like Sink node. (iii) Sink node verified and establish a connection between desired destinations. Before starting the actual authentication protocol between two networks entities, it is necessary to undergo a registration process by every communication party, to retrieve cryptographic credentials that are used for the authentication phase. Figure-1 describe the whole scenario of deployed IOT architecture in which three sites are interconnected and end users can establish a secure communication link between each other. This scheme consists of two stages. In stage one, node establishes secure entering into routing table via strong node authentication like Base Station (BS), Cluster Head (CH) and Sink Node (SN). After successful joining, an end to end session communication will start using Two-Level Session Key(TKS).In a key setup phase, any node can request to join the network by establishing a secret key for secure communication and data transmission. The detail of node association for authentication and establishing level-1 key is shown in table-2 as protocol-I

Table 2: Node Association Phase

Protocol I: Node Association Phase – Smart Phone user ---

IOT Infrastructure

1. $N_C \rightarrow BS$: $K_{N_C-BS}\{ID_{N_C}, S_{nk}, \text{REG}_{\text{REQ}_{\text{CAT}}}, T_{SN_C}, V_{nN_C}, D_{hN_C}, \text{HMAC}\ (ID_{N_C}||T_{SN_C}||\ V_{nN_C}||D_{hN_C})\}$
2. $BS \rightarrow S_{nk}$: $K_{BS-S_{nk}}\{ID_{N_C}, \text{REG}_{\text{REQ}_{\text{CAT}}}, T_{SN_C}, V_{nN_C}, D_{hN_C}, \text{HMAC}\ (ID_{N_C}||T_{SN_C}||\ V_{nN_C}||D_{hN_C})\}$
3. $S_{nk} \rightarrow CH$: $K_{S_{nk}-CH}\{ID_{N_C}, \text{REG}_{\text{REQ}_{\text{CAT}}}, T_{SN_C}, V_{nN_C}, D_{hN_C}, \text{HMAC}\ (ID_{N_C}||T_{SN_C}||\ V_{nN_C}||D_{hN_C})\}$
4. $CH \rightarrow N_S$: $K_{CH-N_S}\{ID_{N_C}, T_{SN_C}, V_{nN_C}, D_{hN_C}, \text{HMAC}\ (ID_{N_C}||T_{SN_C}||\ V_{nN_C}||D_{hN_C})\}$
5. $N_S \rightarrow CH$: $K_{N_S-CH}\{ID_{N_S}, N_C, T_{SN_S}, V_{nN_S}, D_{hN_S}, \text{HMAC}\ (ID_{N_S}||T_{SN_S}||\ V_{nN_S}||D_{hN_S})\}$
6. $CH \rightarrow S_{nk}$: $K_{CH-S_{nk}}\{ID_{N_S}, N_C, \text{REG}_{\text{RPY}}, T_{SN_S}, V_{nN_S}, D_{hN_S}, \text{HMAC}\ (ID_{N_S}||T_{SN_S}||\ V_{nN_S}||D_{hN_S})\}$
7. $S_{nk} \rightarrow BS$: $K_{S_{nk}-BS}\{ID_{N_S}, N_C, \text{REG}_{\text{RPY}}, T_{SN_S}, V_{nN_S}, D_{hN_S}, \text{HMAC}\ (ID_{N_S}||T_{SN_S}||\ V_{nN_S}||D_{hN_S})\}$
8. $BS \rightarrow N_C$: $K_{BS-N_C}\{ID_{N_S}, \text{REG}_{\text{RPY}}, T_{SN_S}, V_{nN_S}, D_{hN_S}, \text{HMAC}\ (ID_{N_S}||T_{SN_S}||\ V_{nN_S}||D_{hN_S})\}$

1. End user using Smart Phone or another device will send encrypted association request using already established a symmetric key to desire sensor via a base station (BS).
2. After receiving this message, BS will decrypt with already symmetric key and after localizing required destination encrypt with the symmetric key to delivering secure on sink node. There are many devices, so message contains category (CAT) which shows that request will forward only for the specific node; like maybe for Temp sensor, surveillance cam, etc.
3. Message Authenticating Code (HMAC) is used against a replay attack. The receiver can verify the parameters by computing HMAC of received data to prove integrity.
4. CH will send request reply having requested data to sink node and sink node forward to BS for the user.

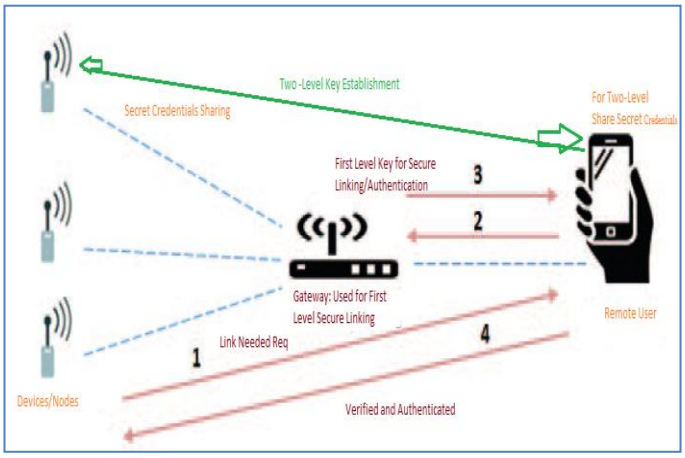

Figure: 2- Network Architecture [29]

The network architecture is mainly composed of the sensor nodes, the gateway node, and the remote user depict in figure-2 has been adopted as real world IoT-based distributed architecture. The proposed communication system enables collected data from a sensor node to be transmitted directly to the remote mobile user after a successful mutual authentication between a sensor node and the remote user.

This process will complete when all steps of protocol-I are performed. The authentication protocols should not only be resistive to malicious attacks but also they should be lightweight for deployed less performing edge devices in IoT scenario. Rather using for generic WSN applications, IoT combined WSN use-cases are currently deployed in smart-home, smart- city, health-care, and industry monitoring applications. Their collected data are used to identify HMAChine abnormalities and to create safety alarms. There can be instances where the users inside and outside the power plants want to acquire raw data directly from the sensor nodes. The end-users and the sensor nodes have to authenticate each other before transferring raw data.

B. Two-level Session Key Establishment

In IoT-based architecture shown in figure-1, assumed that nodes are associated with fool proof strong security mechanisms like Elliptic Curve based symmetric key. Key established via a third party or symmetric key has a chance to forward and replay attack by malicious intruders. It is necessary to propose a technique which makes it independent. We propose a Two-level Session Key (TSK) to make secure and authenticated communication between deployed sensor and end user.

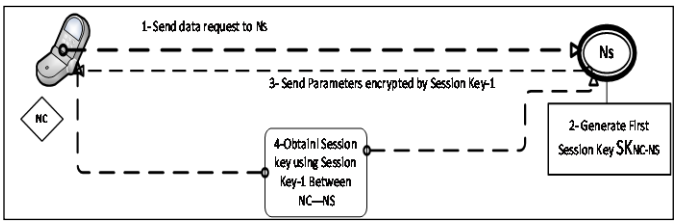

Figure-3 Two-level Session Key for New Session

Two level session key used against replay and Dos attack. It will refresh key for next session. It has a novelty and new technique which establishes a new session key for each new session. It has been assumed that smart phone has been registered and entered into the routing table of BS. For next communication session, data will remain encrypted form and BS and Sink node just forward that encrypted to the sensor node. The next session communication starts as shown in protocol-I and figure-2.

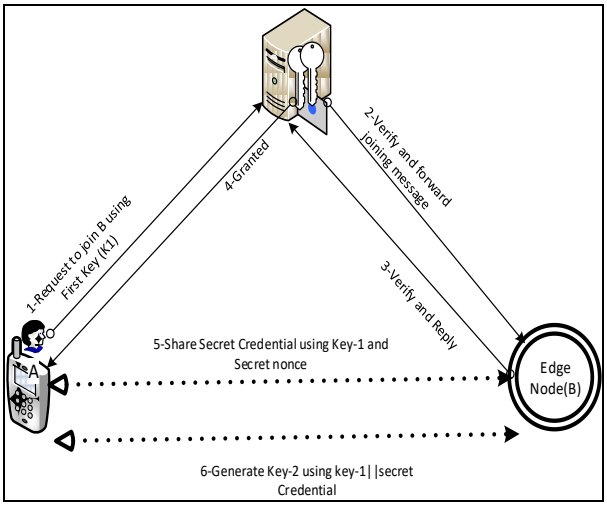

Figure-4: Second level key generation Mechanism

Protocol II: Two-level Session Key-establishment (TSK)

1. $N_C \rightarrow N_S: K_{N_C-N_S}\{ID_{N_C}, \mathrm{SK_{REQ}}, \mathrm{V}_{nN_C}, \mathrm{HMAC}\ (ID_{N_C}||\mathrm{V}_{nN_C})\}$
2. $N_S: SK1_{N_C-N_S} = ID_{N_C} \otimes K_{N_C-N_S} \otimes \mathrm{V}_{nN_C} \otimes ID_{N_S}$
3. $N_S \rightarrow N_C: SK1_{N_C-N_S}\{ID_{N_C}, \mathrm{V}_{nN_S}, \mathrm{HMAC}\ (ID_{N_C}||\mathrm{V}_{nN_S})\}$
4. $N_C, N_S: SK_{N_C-N_S} = ID_{N_S} \otimes SK1_{N_C-N_S} \otimes \mathrm{V}_{nN_S} \otimes ID_{N_C}$

1. Mobile phone (N_C) send data request to sensor node (N_S) and send parameters mentioned in step-1 encrypted by symmetric key established as in algorithm-I. Message Authentication Code (HMAC) used to integrate message. Nonce value by V_{nNc} used by mobile as a nonce number.
2. Sensor node (N_s) and N_C generates first-time session key $SK1_{N_C-N_S}$ using nonce value V_{nN_C} and taking XOR with the existing pair wise symmetric key $K_{N_C-N_S}$ between N_C and N_S as illustrated in step-2.
3. Now N_S uses this session key $SK1_{N_C-N_S}$ to encrypt the message including identity of N_S, nonce value V_{nN_S} generated by N_S and HMAC of these parameters as shown in step-3.
4. Finally N_C and N_S obtain the session key $SK_{N_C-N_S}$ by taking XOR of first time session key $SK1_{N_C-N_S}$ and nonce value V_{nN_S} along with Identities of both nodes.

IV. RESULTS AND ANALYSIS

In this section, a detailed analysis of the proposed authentication protocol regarding performance and security is provided. Furthermore, it is justice why the proposed solution can be deployed on resource-constrained devices in distributed IoT applications. At the end of the section, the authors present the limitations that are engaged with the current proposal and should be improved in future. H.-R [23] every key management schemes should satisfy some conventional security requirements such as validation, freshness, privacy, and trustworthiness. Key management may be a core mechanism to protection the security in network and may be outlined as a collection of processes and mechanism that support key establishment and maintenance in a progress relation between authorized parties according to the security policy The key management in WSNs consists of various processes such as creation, distribution and maintenance of the secret keys. Key management for encryption, which can make data transmission more secure, and at the same time make a less resource utilization, have vital importance in IoT scenario where low power edge devices are performing.

A. Performance Analysis

Recent related key establishment protocol for wireless sensor networks are presented below. Eldefrawy et al. [24] proposed a key agreement algorithm with rekeying for WSNs using ECC and RSA public key cryptography; this protocol is also dependent on a specific routing protocol. As a result, the protocol only establishes a pair-wise key between nodes in a specific route, which avoids establishing a pair-wise key for each of the neighbors. The shortcomings of Eldefrawy et al protocol are that the protocol has to be used with a specific routing protocol and the higher communication overhead due to the use of both RSA and ECC in the key establishment. Using the concept of Wong at al [25] and based on ECC, H.Huang et al in [26] designed a key establishment in the authentication procedure of the access control scheme for WSNs. The new designed key establishment also used the concept of time bound in which once a period has elapsed, the sensor node in the wireless sensor network cannot access any data for a future period to protect future messages. Nevertheless, adversaries can still apply sensor node replication attacks in the period of expiration time ***wi***. The reason being that the adversary can compromise the sensor node and apply a replication attack before expiration time ***wi*** is reached.

I.Hang et al. in [27] designed a new identity-based DH key agreement protocol for wireless sensor networks Based on the Arazi-Qi Scheme, Authors prove that this key establishment scheme is resilient against the masquerade attack, replay attack, and key regeneration attacks Computation resource on sensor nodes according to the performance analysis. In proposed scheme MD5 (128-bits) used for data authentication and data integrity. In [30,31] authors evaluated energy and communication cost using different symmetric cryptography functions. The evaluating function E=P x T is used where; E is the electric energy expressed in joules and P is the nominal power of the electrical dipole expressed in watt. According to their analysis and parameters used in our schemes are as Transmission one-byte energy cost is 5.76µJ, reception one-byte cost is 6.48 µJ, AES-128 used at gateway node for first level session key generation for node authenticity is 42.88 µJ of 16-byte, and computation of HMAC cost is 62.15 µJ. By these assumptions, we evaluate our performance of proposed scheme.

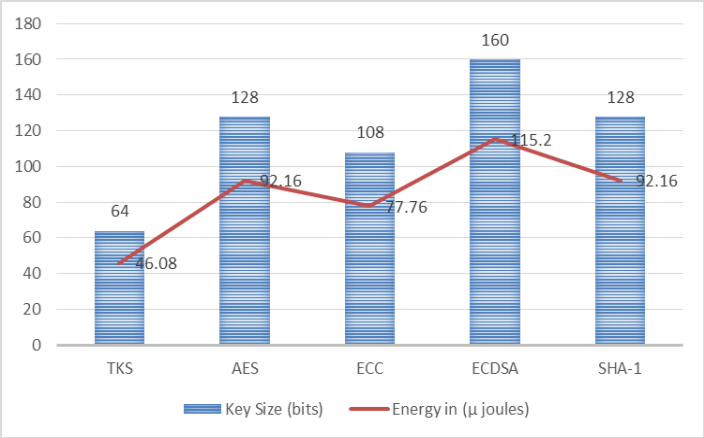

Figure-4 Impact of Key Size on Energy

By above analysis and data, we compare proposed scheme efficiency. We compare key size (in bits) and energy (µ-joules) with proposed schemes as shown in figure-4. The total data used for authentication and session key is 36-byte which is less than already proposed schemes. We use bitwise exclusive XOR

operation size 8-byte one side and 16-byte for a complete round and secure hash function SHA-1, that is 4-byte per operation. By all these sessions, a key size of and consumption of energy during communication is lesser than other schemes as shown in figure-4.

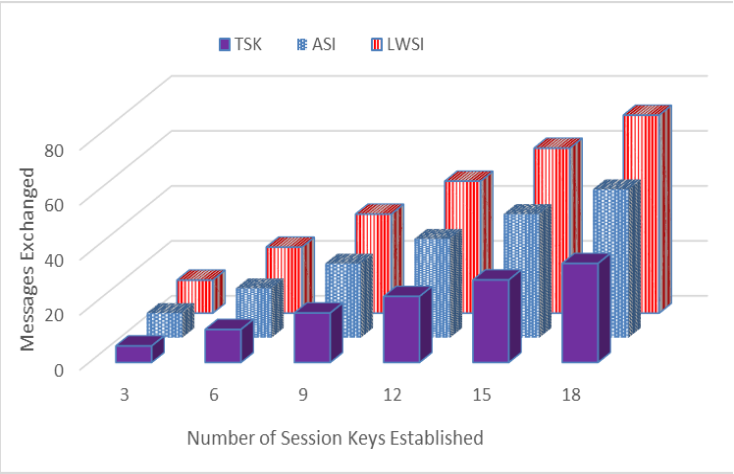

Figure-5 Communication Cost for Session Key Establishment

In proposed scheme the number of share messages also lesser than other schemes. We have compared and results shown in figure-5. The total number of messages exchange for two level sessions key are four in which two used for node secure node association. Verification of node before joining is resisted malicious node accessing in the network. So, by this parameter proposed scheme needs on three messages for one key that is efficient as compared to others on message exchange and communication overhead.

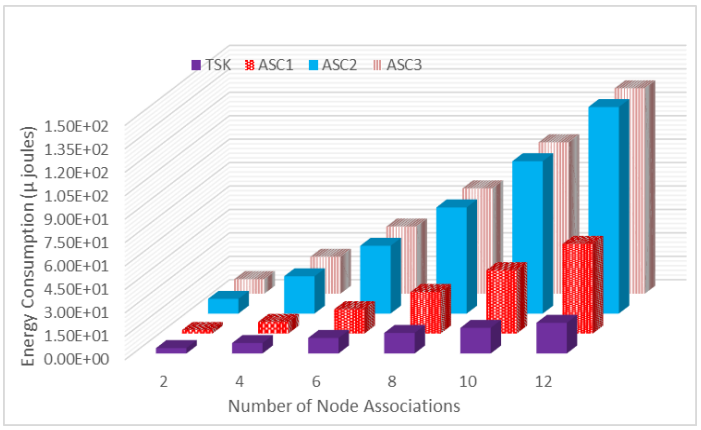

Figure-6 Communication Cost for Node Association in IoT

Figure 4 elucidates the impact of key sizes on energy consumption in different schemes. In this scenario, we follow Kim at al ECC [27] uses a key size of 108 bits and consumes 77.76 microjoules. ECDSA uses a 160 bit key by consuming 115.2 microjoules. In comparison, the proposed TKS scheme consumes only 46.08 microjoules with a key size of 64 bits is used to encrypt data between both ends and the procedure to generate a key based on two level of challenge-response process. Total energy cost is calculated as the sum of computation and communication cost for message authentication code (HMAC), encryption and hash of data. We estimate the cost of our TSK requires to transmit and receive a single bit by consuming 0.72µJ and 0.81µJ respectively. During the listening mode, only 0.29µJ are consumed. HMAC computation requires 23.09µJ. For the total cost calculation, we consider the cost of transmission, reception, listing and cryptographic operations.

B. Security Analysis

Our proposed scheme achieves robustness against the following attacks; Mutual authentication is supported in our scheme where users authenticate themselves before accessing data, and also the coordinator proves its authenticity. This allows avoiding impersonating the coordinator as an attacker can impersonate the coordinator to send false data to users. Therefore, users are sure about the authenticity of the received data. In our scheme, at the end of a successful authentication the sensor node and end user establish a secret key. This key can be used as a session key to secure the communication between the two entities including user and the deployed sensor/device. Some proposed scheme [28] such as avoid replay attack by adding a timestamp to every sent message. This time-stamp guarantees that the message is fresh and therefore is not an old replayed message. However, one of the disadvantages of using a time-stamp is that it requires synchronization between entities. In our scheme we provide this security service (freshness of message) by using the concept of the nonce and two-way session key therefore synchronization between entities is not required. Brute force attack: According to the proposed protocol, it is difficult to find the correct session key. Because our scheme based on two ways session key and keys change every time at the completion of the transaction. Replay attack prevention: By using a nonce and limited-use session keys, the proposed protocol can prevent replay attack as the session keys used in this protocol are used only once. Data Integrity: The integrity of data is satisfied by using a hash function. Party Authentication: The proposed protocols can ensure party authentication based on Message Authentication Code (HMAC) with shared key between sender and recipient to ensure the parameters are not altered or changed. Man in the middle attack: An attacker who pretends to be an authorized party is not able to analyze the transmitted message since the session keys used in our protocol are constantly changed by using strong encryption technique. Replay attacks not possible because of new nonce are generated for such authentication to provide mutual authentication. HMAC is generated at the node using their identities, so there is not possible impersonate a node. Randomly nonce number generation process defend for denial of services and two level key generated by agreement of gateway/central authority. The identity of both end proven by a central authority and in our scheme ECC used for this process that has enough security for masking their IDs a mutual authentication. Scalability and session key establishment have robustness property because a central authority has added a new node and our scheme has two level of communication, so the one node failure and dependency limitation have solved.

C. Motivations

Elliptic Curve Cryptography (ECC) has ascended as an intriguing methodology contrasted with RSA-based algorithms. Are more energy saving and less key size for the same level of security. IoT applications are utilizing ECC based certain technique. It offers a less energy utilization and calculation overhead. It utilizes cryptographic operations, for example, exclusive-OR (XOR), hash function, and symmetric cryptography. This class is frequently known for its high energy saving. For this reason, authors in having proposed a client verification and key assertion plan given the IoT thought for heterogeneous specially appointed WSNs [29]. It utilizes just cryptographic operations between a remote client, a central hub, and an edge device. It ends by a

foundation of a secret shared key connecting the remote client and the sensor node. Recently, authors in [30] proposed another validation scheme. The scheme commences another technique with safely send messages to the verification stage. The traded messages are sent ensured by an HMAC. The HMAC calculation depends on sensor node identity without sending the secret identity of the planned message. The investigations demonstrate that the proposed plan is delegated lightweight since it gives confirmation less vitality utilization.

V. CONCLUSION

The proposed TSK scheme is a two level authentication mechanism in which end users independently established session key in two ways. The aim of proposed scheme is to resist against reply, channel, forward and key regeneration attack and make secure communication with end users in the IoT-based scenario. Highly resource-constrained nodes are then able to establish a shared end-to-end secret with any remote entity, making use of symmetric cryptography in a new fashion. This is achieved through simple exchange with strong relay nodes like Base Station, Sink Node, and Cluster Head during node association phase. HMAC, nonce, secret credentials and XOR symmetric functions use which are lightweight and provide enough security in our IoT-based end user secure communication. TKS has been compared with existing symmetric key schemes and show better on memory and energy consumption. We have evaluated our protocol regarding both security aspects and energy cost savings. The results regarding security our scheme is secure and effective.

Acknowledgment

This work was funded by the National Natural Science Foundation of China (61471035), and Fundamental Research Funds for the Central Universities (06105031, 06500010). In particular, it was supported by Cybermatics and Cyberspace International Science and Technology Cooperation Base.

REFERENCES

1. R. Roman, J. Zhou, and J. Lopez, “On the Features and Challenges of Security and Privacy in Distributed Internet of Things,” Computer Networks, vol. 57, no. 10, pp. 2266 – 2279, 2013.
2. S. Raza, D. Trabalza, and T. Voigt, “6LoWPAN Compressed DTLS for CoAP,” in Proceedings of 8th IEEE Conference on Distributed Computing in Sensor Systems (DCOSS), 2012, pp. 287–289.
3. T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, and G. Carle, “DTLS based security and two-way authentication for the Internet of Things,” Ad Hoc Networks, ELSEVIER, 2013.
4. M. Brachmann, S. L. Keoh, O. Morchon, and S. Kumar, “End-to-End Transport Security in the IP-Based Internet of Things,” in Proceedings of the 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1–5.
5. R. H. Weber, “Internet of Things New Security and Privacy Challenges,” Computer Law and Security Review, vol. 26, no. 1, pp. 23–30, 2010.
6. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
7. S. A. Camtepe, B. Yener, Key Distribution Mechanisms for Wireless Sensor Networks: A Survey, Technical Report TR-05-07, Rensselaer Polytechnic Institute, 2005.
8. Y. Wang, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks, IEEE Commun. Surv. Tutorials 8 (2) (2006).
9. R. Roman, C. Alcaraz, et al., Key management systems for sensor networks in the context of the Internet of things, Int. J. Comput. Electr. Eng. (2011) 147–59.
10. R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, “Key management systems for sensor networks in the context of the internet of things,” Computers & Electrical Engineering, vol. 37, no. 2, pp. 147–159, 2011.
11. Thesis: Collaborative Security for the Internet of Thing, Yosra Ben Saied. <http://www.theses.fr/2013TELE0013> (accessed November 2013).
12. Gartner Inc., Forecast: The Internet of Things, Worldwide, 2013.
13. Nguyen, K.Thuat, M. Laurent, and N.Oualha. "Survey on secure communication protocols for the Internet of Things." *Ad Hoc Networks* 32 (2015): 17-31.
14. G. Piro, G. Boggia, L.A. Grieco, A standard compliant security framework for ieee 802.15.4 networks, in: Proc. of IEEE World Forum on Internet of Things (WF-IoT), Seoul, South Korea, 2014, pp. 27–30.
15. I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Commun. Mag. 40 (8) (2002) 102–114.
16. G.Sharmam, S. Bala, A.K. Verma, Security frameworks for wireless sensor networks-review, in: 2nd International Conference on Communication, Computing & Security, ICCCS-2012, 2012, pp. 978–987.
17. J.-Y. Lee, W.-C. Lin, Y.-H.Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next-Generation Electronics, ISNE 2014, Kwei-Shan, 2014, pp. 1–2.
18. M. Turkanovi, B. Brumen, M. Hlbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion, Ad Hoc Netw. 20 (2014) 96–112.
19. N. Ye, Y. Zhu, R.-C. b. Wang, R. Malekian, Q.-M. Lin, An efficient authentication and access control scheme for perception layer of internet of things, Appl. Math. Inf. Sci. 8 (4) (2014) 1617–1624.
20. He, Debiao, Neeraj Kumar, and Naveen Chilamkurti. "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks." Information Sciences 321 (2015): 263-277.
21. R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, “Key management systems for sensor networks in the context of the internet of things,” Computers & Electrical Engineering, vol. 37, no. 2, pp. 147–159, 2011.
22. L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002, pp. 41–47.
23. H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks."
24. Eldefrawy, Mohamed Hamdy, Muhammad Khurram Khan, and Khaled Alghathbar. "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography." 2010 International Conference on Anti-Counterfeiting, Security and Identification. IEEE, 2010.
25. Wong, Kirk HM, et al. "A dynamic user authentication scheme for wireless sensor networks." IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06). Vol. 1. IEEE, 2006.
26. H. Huang, A New Design of Access Control in Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 2011, doi:10.1155/2011/412146.
27. I. Hang, M. Ullmann, and C. Wieschebrink, A new Identity-based DH Key-agreement Protocol for Wireless Sensor Networks Based on the Arazi-Qi Scheme. In WiSec'11, Hamburg, Germany, 2011: ACM
28. Kim, Daehee, Dongwan Kim, and Sunshin An. "Communication Pattern Based Key Establishment Scheme in Heterogeneous Wireless Sensor Networks." KSII Transactions on Internet & Information Systems 10.3 (2016).
29. Tang, Ssu-Wei. "A Lightweight Continuous Authentication Protocol for Internet of Things." (2016).
30. H. Khemissa and D. Tandjaoui, “A lightweight authentication scheme for e-health applications in the context of internet of things,” in Next Generation Mobile Apps, Services and Technologies (NGMAST), 2015 Ninth International Conference on. IEEE, 2015, pp. 90–95.
31. G. De Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, “On the energy cost of communication and cryptography in wireless sensor networks,” in Networking and Communications, 2008. WIMOB’08. IEEE International Conference on Wireless and Mobile Computing,. IEEE, 2008, pp. 580–585.
32. J. Lee, K. Kapitanova, and S. H. Son, “The price of security in wireless sensor networks,” Computer Networks, vol. 54, no. 17, pp. 2967–2978, 2010.