A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications

Maria Almulhim, Nazurl Islam and Noor Zaman

Department of Computer Sciences, Computer Sciences and Information Technology College, King Faisal University, Hofuf, Saudi Arabia

Abstract

Internet of Things (IoT) indicates to a network, which consists of physical objects able to collect and sharing electronic information. IoT contains a wide set of “smart” devices and sensors which transfer data at the network through IoT applications. The rapid expansion of IoT and wireless technologies lead to finding new opportunities for growth in various fields such as Education, Transportation, Agriculture, and especially in the Healthcare sector. However, the growing use of IoT services, especially in E-health applications will increase security challenges, such as authentication of several connected objects and exchanged data. Due to the sensitivity of e-health applications, the aspect of authenticity is one of the most significant challenges, which should be addressed effectively. Therefore, E-health applications require an authentication scheme to protect data transfer, use and exchange between sensor nodes and Base Station. E-health applications are prone to several hacks, and this is due to all communication occurred through a wireless medium. Furthermore, IoT has low capabilities components in computing and energy resources. So, one of the major goals of building security protocols is to improve using of the network, which allows sensors to save energy and lead to extend the network’s lifetime and to be resistant against several types of attacks. At this research, we are proposing an efficient secured group-based lightweight authentication scheme for IoT based E-health applications; this scheme authenticates and establishes secure channels through sensor nodes and Base Station. The proposed scheme with a feature of the group-based node will reduce distance and consumed energy, as well as leads to reduce communication cost. In addition, it will be resistant against hacks by using elliptic curve cryptography (ECC).

Index Terms:

E-health applications; Authentication; Lightweight; Group-based node; Energy; ECC.

1. Introduction

With the IoT, nowadays it is considered as one of the most important, newest and fastest spreading mechanisms in the communication area. IoT is consisted of devices and integrating sensors at daily smart objects that linked to the Internet through wireless sensor networks that lead to open the door to new methods of exchanging the data which were not potential before. IoT has several applications and one of the most effective is E-health applications, e-health applications are radio-frequency that based on wireless networking technology and consist of wearable sensors which connected to Base Station [1]. Currently, a great number of researches are learning IoT applications at e-health field. E-health term had been recently established which handles management of healthcare with the backing of electronic communication and processes techniques. E-health systems such as wearable devices and cell phones provide continuous monitoring of patients. Thus, this will provide many advantages like cost saving, transportation, and insurance costs and health care provider. Therefore, this will lead to achieve the goal of facilitating secure interactions among healthcare providers and patient, which leads to better quality of healthcare, and save the time of patients [2]. E-health applications are an exhibition to hack data and increasing issues at issues in security aspects due to rising a number of access points and critical data through E-medical records as well as the growing of use wearable technology [3]. So, one of the main issues of IoT is the high level of security that needed to keep all communications secured. The concerns of security are extended due to the rapid deployment of IoT [4]. At IoT, Security is mainly part of E-health applications, which provide a high level of security for medical data [5]. There is a need for more efforts and more researches to handle security problem. However, many of researchers had searched about an open issue at IoT [6]. Researches aim to meet the requirements for making security a major factor to build IoT E-health applications to protect data communication mechanisms [7]. Based on the above brief discussion, our paper is proposing an efficient secured group-based lightweight authentication scheme for IoT based E-health applications. The proposed scheme will be resistant against several types of hacks. Also, with a feature of the group-based node will reduce distance and energy and as well as lead to reduce communication cost. At the beginning, we discuss briefly IoT security challenges, especially at E-health applications. The rest of the paper ordered in four parts. In section II, we present Literature review. In section III, we proposed our scheme and explained it in detail. In section IV, we discussed and presented results analysis. Finally, Section VI, we end with the main contributes to this paper.

Manuscript received January 5, 2019
Manuscript revised January 20, 2019

2. Literature Review

This section will briefly discuss the literature review mainly in the authentication and security area for IoT E-health based applications. After that, I will list a summary of comparisons of related studies. In a study [2], the effects of IoT in establishing of E-health successfully and indicating, the barriers that will contribute to reducing the chance of successful deployment of IoT-based e-health applications have been analyzed. Considering the adoption of Big data, cloud computing and implementation of IOT that may improve the health-care industry in several benefits: help the patient by reducing cost and need of visiting the hospital physically, health care provider cost, human resources and finally transportation costs which will contribute directly to improve the quality of health care. Barriers that should be focused on in order to have successful adoption of IoT base E-health are security, privacy as they will become big vulnerable especially in open networks. A study [3], they discussed the recent topics and issues related to the E-health applications, and how developers and programmers deal with them. These security issues came from wide use and rapidly evolve of IoT e-health systems. After that, they specify the causes and what is the proper solutions to minimize them. Later, they will discuss what may occur in future regarding security and privacy issues and how to handle them. Finally, they list some other issues such as Smart health and cities, Cloud computing, Biometrics, and social networks. They noted that these mentioned problems are out of their study limits and will consider them in the future. A study [8], they offer a technique that it’s good to use in a healthcare environment due to their need to less power, this technique is Narrowband IoT (NBIoT). In addition, they consider it good for E-health system because it's unified. The big challenge of this technique is security. In addition, there is another issue, which is absent; offering service at the needed time. Therefore, this may prevent using it at E-health applications. Because of above the reason, they offer a solution by using Constrained Application Protocol (CoAP) and IPv6 through 6LoWPAN. A study [9], they offer secured model, that help to minimize problems related to security and how we take advantages from wearables. They also offer various areas of mechanisms of architectures of IoT e-health and how it assists to provide easy access and sending and receiving e-health data. In addition, they present precise search regarding how e-health applications of IoT deal with several patient’s healthcare services. A study [10], they searched and studied IoT nodes and offer virtual network cloud system security framework. one of the main defects of cloud networks of IoT are the issues of nodes usage over virtual network cloud system. These nodes can be connected but they need surveillance from a Cloud Service Provider (CSP). CSP need to take attention from malicious node because of they not able to be disconnected from the network. They offer protocol with secured key management for clients and CSP. After that, they established a technique for lightly weighted cryptography which offers a protocol for key exchange and able to build a secured connection for nodes. They used Diffie-Hellman algorithm because it offers variety benefits such as less power consumption, robust and lightweight. The authors in [11], search about the major problems that occurred at the usage of IoT E-health applications. They discussed how to offer the best solution for surveillance of patients with the inveterate disease by using REMOA project. This project collects data from multiple sensors, this leads to offer needed safety for IoT e-health. But there are still some issues need to be fixed at this project, such as non-attendance of infrastructure authentication of transmitting data. At this paper [1], they provide a scheme for an E-health application which is light weighted and authenticated. It will be led to protect health information by applying an authentication feature for Base Station and Sensors. To achieve authentication exchanges integrity; they depend on nonces and Keyed-Hash message authentication (HMAC) at their scheme. Based on the results of their scheme; it shows that its maintained energy pulses its resistance against several attacks. At future, their goal is to evaluate their protocol in the realistic case to get more results about consumption of memory and time execution. This paper [12], presented mechanisms for encrypting, sign and authenticate communications of medical devices which are: a collection of cryptographic Subscriber Identity Module (SIM) card. The goal of this study is to handle the problems that present at IoT, which lead to robust, fixed and secured technology to make IoT be realistic at healthcare provider environments. So, they offer RFID/NFC and they consist of cryptographic SIM card to improve safeness, and they developed a protocol to mobility for 6LoWPAN. Thus, they focus on some of the schemes to handle issues that face IoT at healthcare areas. At future, they are planning to introduce specific algorithms to know more about characters of architecture that established chronobiology algorithms and health science. In this paper [13], they discussed various issues that related to IoT E-health applications, such as remote surveillance of elderly pulse privacy and security. All of them connected to e-medical information records. The surveillance of patient's data is to protect their confidentiality and prevent non-ethical use of their data. As we know, wireless communication leads to weakness of transmitting data because of the open property of wireless networks. Therefore, the data under high risk and it can lead hackers to misuse data. We can reduce that by using (HIPAA) health insurance portability accountability act. This paper [14], offers an evaluation for IoT adaptive security, which uses current products and software for open resources, this project, called: Security Adaptive for Smart IoT in eHealth (ASSET). In addition, they discussed learning how the orientation of the antenna effect on the consumption of energy. Therefore, they introduced and developed an approach of rating of consuming energy that used the process of Holt-Winters by guessing. This will be beneficial if they want to know the more secured lightweight solution of ASSET project. In future, they will evaluate security algorithm consuming of energy performance and communication prices by using their testbed. This paper [15], focuses on IoT E-health which covers specifically the level of security and searches their advantages of network and protocols. Smart Health-NDNoT, present how to ensure the security of data instead of linking security and this is done by applying some attempts from Named Data Networking (NDN). UT-GATE interest in security level, precisely at the establishment of the architecture of gateway and network. A project of Fault Tolerance focuses deeply on the architecture of the network, real-time and skillful system. In addition, there are extra efforts of studies that work over current security protocols. In their future work, they plan to add more solutions for IoT E-health techniques. At this study [16], to block facing issues at distributed IoT applications, they present framework secured, which applies secured adaptive contexts to help with the right monitor information. This will be led to follow data and meet responsibility; also, it involves taking legal responsibility. The main idea to have the privacy of E-health data is to execute a secured context linked with each resource. Therefore, at any establishment of data; the secured context needs to be automatically generated. At this study [17], they are prepared to select solve AKA which is good for IoT environment, and this can apply by test schemes free-escrow lightweight that provide benefits for performance and safety plus consumption of power. In addition, they confirm and offer a collection of certificates implicit plus strengthened-Menezes-Qu-Vanstone (SMQV) which result in lightweight and secret protocols. As they said, if you want longer network life; design secured schemes of WSN for a network using improvement and handling and protect energy. In fact, even when they said that schemes of AKA more effective than SMQV, but later it presented some security errors. Therefore, it’s not easy to add ant refinements to SMQV. In this paper [18], there are some protocols as if Transport Datagram Layer Security (DTLS) premise on some ethics of internet field that used and proposed at this paper, which is the execution of whole scheme of implementation of two way secured authentication for IoT. They used DTLS handclasp authentication that based on RSA keys to implementing the verification. They offer an algorithm that always used public key cryptography, which relies on RSA, and module of security depends on it. They found that it can be applied through broad at the platform of hardware which is appropriate with IoT, so they discover that after applying it over DTLS. This wide support is relying on systems of the internet of things. Therefore, their proposed scheme supply privacy and authenticity, integrity of SMS plus end 2 end latency, memory prices and minimum power. Finally, they conclude that the best solution for safety to evolve IoT is the usage of DTLS. A paper [4], they proposed a method of encryption depend on XOR manipulation, instead of using the hash function because it’s complex encryption, using this will lead to prevent counterfeiting and protect privacy. The absence of cryptography in RFID is the main challenge in designing security. When RFID connect to the internet, the items of tags will move through many readers fields after that, linked to RFID communication protocol. Therefore, due to RFID not having anti-counterfeiting features, hackers can scan EPC from the tag. Therefore, their proposed lightweight cryptography protocol can solve this issue and their simulation results show that they can improve it, also this protocol can be used to build procedure to mutual authentication of RFID for IoT applications. At this paper [19], they proposed energy-efficient, lightweight and robust security protocol for Wireless Sensor Networks (WSN) systems. As we know, at WSN if there is any new device will link to the network, initially, it needs to ensure mutual authentication step. After that, establishing a secured and protected channel to protect transmitted data. Therefore, at their work, they implemented the secured protocol with lightweight and energy efficiency features, which lead to protect most WSNs. In addition, it will guarantee mutual authentication of communication objects and secured privacy and secrecy of transmitted data. The technique of personalization will fix the issue of internal identity usurpation. This protocol offers lightweight and robust security encryption symmetric algorithm (CCM/AES GCM) and this leads to a very rapid build of a secure channel. In the end, this protocol is resistant to replay attacks and cryptanalysis. At this paper [20], they suggested secure authentication and key management protocol, with the usage of hybrid cryptography which includes certificate-less and symmetric cryptographic public key algorithms. Their performance comparison results and evaluation present that they are able to meet the requirements of security at IoT e-health sector. We know, one of the main challenges at the environment of networking IoT is constrained resources. Based on that, they suggested mutual authentication protocol build key through sensor node resource constrained at IoT e-health areas and entity of remote users that linked to IoT over the internet. This protocol usage Key Generation Center (KGC) that it's not necessary to be completely trusted. Their protocol is lightweight which has low computational cost and low overhead message. Based on their mathematical analysis; their protocol shows that it's secured and protected against various attacks in IoT. In this paper [21], they offered a lightweight and efficient secure authentication protocol for IoT. They challenged and showed that Amin et al. protocol is weak against DoS attack and replay attack; this protocol used three factors key exchange authenticated for WSN. Based on these weaknesses in that protocol, they implemented their protocol. They did analysis and found that their protocol is effective. In this paper [22], they proposed a model of Capability Based Access Control (CBAC) Elliptic at Curve Cryptography (ECC) based on Mutual Authentication to guarantee secured authorization. AVISPA tool used to evaluate the protocol, which is a tool of verification, and protocol of security; they found that it's protected against attacks when using EMA and CBAC. They also did analysis about consumption of power through several models, and they found that their mechanism is energy-efficient for application of IoT. The presented method based on ECC led to high scalability, low memory requirement and facilitate deployment through an environment of IoT. To meet mutual authentication, it provides for sensors low communication overhead. Based on their test through the tool of AVISPA, they found that it could be resisted against DOS attack, replay attack, capture attack of the node and man-in-middle attacks. At this paper [23], they discussed how important Mutual authentication for applications of Smart City and IoT. It ensures authentication of data and offers protection security for users. As we know protocols of conventional mutual authentication are inefficient, not cheap devices of limited resources. At this paper, they offer lightweight encryption public key scheme and protocol of Mutual authentication. This scheme is balanced among the cost of communication and efficiency and the most important point that it meets a high level of security. They did their evaluation of scheme by using Contiki Cooja simulator and platform hardware CC2538. The results of their test present that their scheme is 7 times quicker than ECC and RSA through 112 bits level of security. The time of mutual authentication can be decreased if they enabled offline and online technique. At future, they will do their evaluations at real hardware environment and will apply more improvements on a protocol, which lead to increase message size without any effect on the size of ciphertext. Their scheme includes four algorithms: Setup the system: it turns on the algorithm setup of the system of the scheme encrypted proposed. It generates the key; it turns on the algorithm of production of key Generated the key of the scheme encrypted proposed. Initialization gets IDs and share keys of two devices then swap sharing keys and IDs. Authentication both of two devices execute mutual authentication. At this paper [24], they presented protocols for IoT, which are secured, and lightweight, plus peer authentication protocols, lightweight encryption, authentication data origin and management of key. Protocol of key management is depending on some previously proposed schemes, and they confirmed that they are secured and efficient computationally. In addition, for data they can be encrypted by using their own key randomly. This proposed protocol can implement at applications of IoT instead of using algorithms of whole IPsec set or core IPsec to meet security with high grade plus consumption of low resource, which assists to keep sustainability and performance of the system. In this paper [25], initially, they discussed the architecture of distributed IoT. After that, they analyzed and designed protocol mutual authentication between two sensors at IoT environment. When they compare their protocol to others, their protocol is less lightweight than others are, but on the other hand, it has more features, such as authentication of sensors is including mobile modes and stationary. In addition, there are no limitations of sensors. In future, they plan to apply trust for the current protocol. At this study [26], the main reason for this work is to authenticate the security of remote e-health. Because of limitations of the resource at medical sensors, it’s not possible to use cryptography traditional at IoT based e-health. So, they offer for IoT e-health systems a scheme, which is lightweight and authenticated by using a crypto hash function, identity mask and symmetric cryptography for several exchanges. When they compared it to others, they found that their scheme has a high grade of security, computation, and communication with low cost and end with establishing a key session. Their scheme is appropriate to be implemented at e-health applications. At this paper [27], they presented a collection of e-health security mechanisms and protocols of a secure architecture, which can spread them easily over platforms of mobile, which led to control medications; this is supported by IoT RFID technology. As we know about medications order cycle, doctors start to order prescription, so architecture will protect patient record secured and update events of the patient. Therefore, pharmacist, nurse and health provider can’t change the prescription. They present and evaluated analysis security of Protocol of M-Health Security (MHSP), which provides channel secured for interactions between server and client, which led to powerful authentication. So, as mentioned the usage of RFID tags plus group RFID protocol and Protocol of M-Health Security; offer a completely secured framework to execute Control Medication of E-Health Applications for mobile. This work is suitable for components and architecture of e-health service. At this paper [28], they presented the protocol of Key Agreement and Authentication like Sima’s protocol. They discussed Sima’s and they show how it weak is. Therefore, they entered some improvement to the scheme of Simas. They created formula M1=h(Ri)+IDi, the hackers can’t calculate Ri over IDi and M1. Therefore, they proved how their scheme is protected and powerful against attacks. In this paper [29], they presented a scheme of selective authentication group and usage technique of threshold Shamir. The feature of selectivity, which provides users to choose some of the things that can be accessed later, so the users can gain authority to access selected thing at any time. At below, we can see that their scheme meets the requirements of security with two algorithms: you can easily build secret key; if you know t or anything sharing by t. However, you cannot build secret key in case if you know less than t-1. Therefore, their scheme can offer authentication of the user for several things and authority of access to be secured IoT health-based applications. Based on their discussion, they said; their scheme is the initial that combined authentication group plus selectivity at environments of IoT. In addition, it improves efficiency and security due to a respective feature. Thus, it can be implemented helpfully for IoT health-based applications.

3. Proposed scheme

This section provides a detailed description of the proposed scheme, which is consisted of sensor nodes that distributed around the body of human and single group node linked to Base Station (BS) then server finally to a healthcare provider, ex: E-health applications.

A. Network model

The main architecture of the network is containing wearable nodes sensors, single group node, Base Station (BS), and Server (see Figure. 1). Every node sensor gathers patient vital signs then the group node collects all gathered data from nodes sensors. After that, group node forward information to a Base Station (BS) that can be a portable device then to the Server, using wireless interfaces, such as Wi-Fi or Bluetooth.

B. Lightweight scheme flow diagram/sequence diagram

The below flow chart and sequence diagram as shown in Figure. 2 and Figure. 3 explains the whole workflow of our proposed secured authenticated lightweight scheme; it will start at the side of the patient and if sensors nodes able to communicate with a group node and receive authentication scheme or not. After that node, registration phase will be initiated over group node with Base Station to establish a secure channel. Then, as we mentioned before group node will gather data from sensors nodes to Base Station, then forward them to the server and finally to a health provider. The presence of group node at out proposed scheme and handle the process of registration phase and it will decrease channel distance of sensors nodes and lead to reduce consumed energy, secured communication. In addition, enhanced efficiency of scheme (it explains in detail at below section).

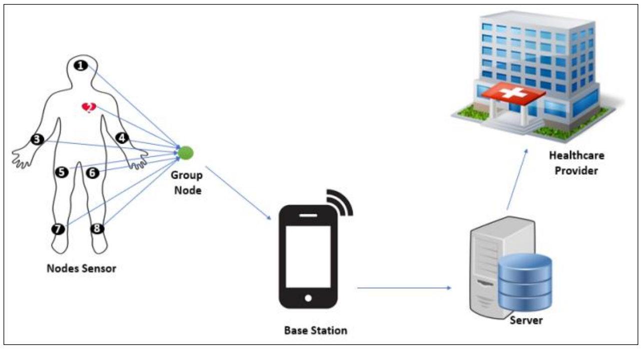


Fig 1. Network Architecture

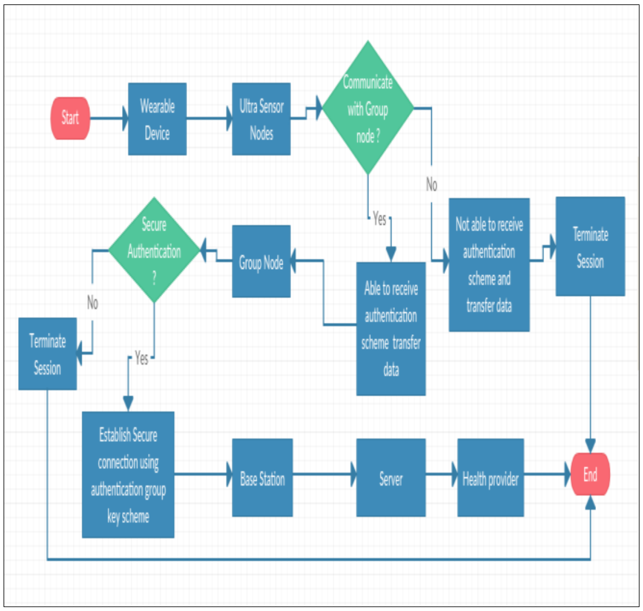

Start
Wearable Device
Ultra Sensor Nodes
Communicate with Group node ?
No
Yes
Not able to receive authentication scheme and transfer data
Terminate Session
Able to receive authentication scheme transfer data
Group Node
Secure Authentication ?
No
Yes
Terminate Session
Establish Secure connection using authentication group key scheme
Base Station
Server
Health provider
End

Fig 2. Scheme flow diagram

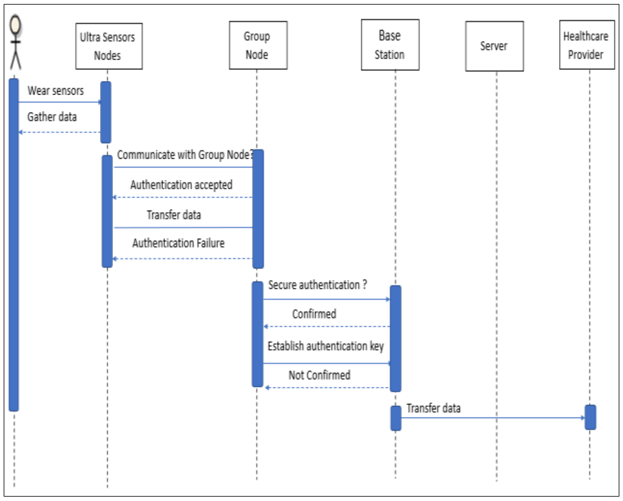


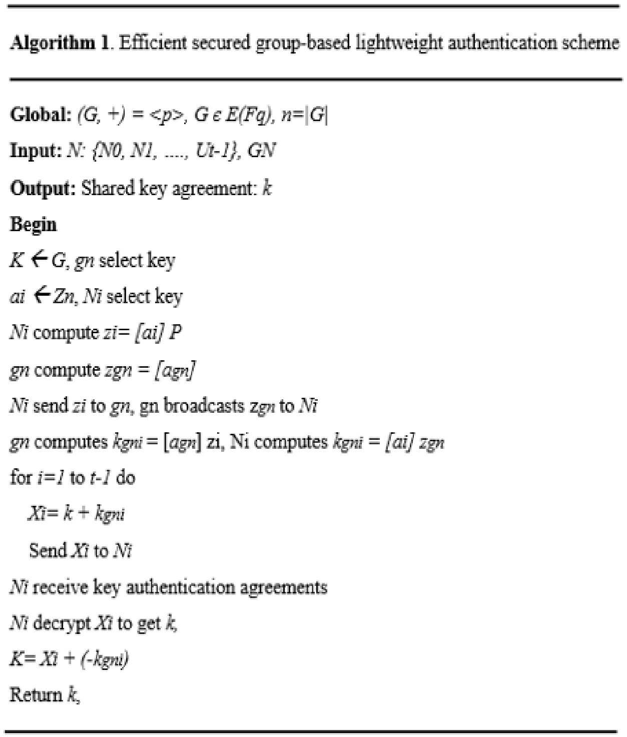
Fig 3. Scheme sequence diagram

C. Lightweight scheme scenarios

At first, we will discuss the scenario if there is no application of group node, if sensor nodes directly forward all data to Base Station then to the server. This will produce several channels because each node will establish its own connection to the base station and they will be prone to attacks and security will be reduced. In addition, due to far distance between sensor nodes and the base station, this will lead to consume more energy and reduce the lifetime of nodes. In addition, the process of key authentication will increase, because if we have eight sensors nodes; they will authenticate eight times to get key from the server, so it will be costly. In our proposed scheme, we are trying to address this issue by applying group node as interface in-between sensor nodes (ultra-sensors) and the base station. These sensor nodes send collected data to group node then group node forwards all data to Base Station then to the server. This will reduce the distance that established between sensor nodes and group node. Therefore, this will reduce energy consumption and increase the lifetime of nodes. On another hand, it will increase security because there are no long distances and will reduce the probability to attack. In addition, it will reduce the key authentication process, because just group node that will authenticate one time to get key from the server, so it will save costs. In this part, we will present a comparison between the two scenarios of our scheme, which will both of them apply and run through simulator (Contiki Cooja).

Algorithm 1. [efficient secured group-based lightweight authentication scheme for IoT based E-health applications], which adopted from Elliptic Curve Burmester-Desmedt 2 (BD) [30,31], the Elliptic Curve BD is the execution of the BD key exchange using ECC. BD protocol performs key exchange in a group of t > 2 participants. Elliptic curve cryptography (ECC) is an approach to cryptography of public key, which depends on the algebraic structure of elliptic curves through finite fields. ECC is the best solution to provide security. The best feature of using BD protocol is its simplicity; where all operations are symmetric and executed through the same protocol with few controls of the data structure.,Our algorithm is focused on key agreement generation and sharing by Group node to other ultra-sensors nodes. Group node key will share the common key agreement among all ultra-sensor nodes and each node does not require communicating separately to get the authentication key for itself.

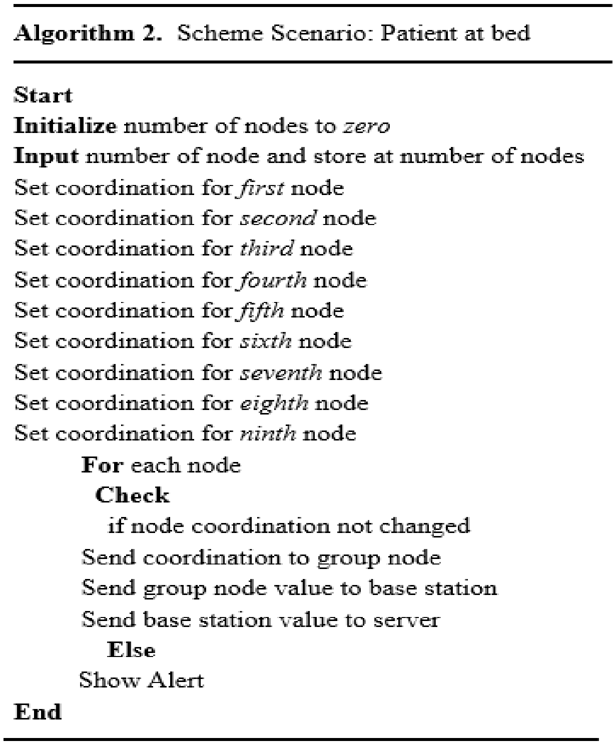
As presented by Algorithm 1, given a finite cyclic group with elements (G; +) = <P>, G ϵ E(Fq), n=|G|, where G is a generator of a set of curve points on field and n is the order number of generators. At beginning of algorithm, each sensors nodes (Ni) select private key (ai) and group node (gn) select private key (agn). Then Ni computes the value of zi then send value to gn. Then gn compute the value of Zgn and broadcast it to Ni. After that, group node computes shared key by using its own private key that chosen before with the exchanged value from other sensors nodes (kgni = [agn] zi, and kgni = [ai] zgn). Finally, each node sensors receives the encrypted shared key Xi = k + Kgni, then they can decrypt it to K= Xi + (- Kgni).



Algorithm 1. Efficient secured group-based lightweight authentication scheme

```
Global: (G, +) = <p>, G ϵ E(Fq), n=|G|
Input: N: {N0, N1, ...., Ut-1}, GN
Output: Shared key agreement: k
Begin
K ← G, gn select key
ai ← Zn, Ni select key
Ni compute zi= [ai] P
gn compute zgn = [agn]
Ni send zi to gn, gn broadcasts zgn to Ni
gn computes kgni = [agn] zi, Ni computes kgni = [ai] zgn
for i=1 to t-1 do
    Xi= k + kgni
    Send Xi to Ni
Ni receive key authentication agreements
Ni decrypt Xi to get k,
K= Xi + (-kgni)
Return k,
```

Scenarios 1: Patient in Bed. As shown in Figure.4, we have a group node and eight sensor nodes, which distributed around the body of the patient (located in bed) to gather general vital signs, such as Temperature, Blood pressure, Pulse, respiration and so on. These sensors nodes send gathered data to group node then group node forwards all data to Base Station then to the server. In this case; the patient will be in bed and will move slightly. Therefore, the group node will be a constant and wearable sensors node will have limited mobility and move with patient movement. Algorithm 2 in below, shows scenario when patient in bed “No mobility status” and set eight sensors node around the patient body with different coordination, then forward their values to the group node and then base station and finally to the server.



Algorithm 2. Scheme Scenario: Patient at bed

```
Start
Initialize number of nodes to zero
Input number of node and store at number of nodes
Set coordination for first node
Set coordination for second node
Set coordination for third node
Set coordination for fourth node
Set coordination for fifth node
Set coordination for sixth node
Set coordination for seventh node
Set coordination for eighth node
Set coordination for ninth node
        For each node
          Check
            if node coordination not changed
        Send coordination to group node
        Send group node value to base station
        Send base station value to server
            Else
        Show Alert
End
```

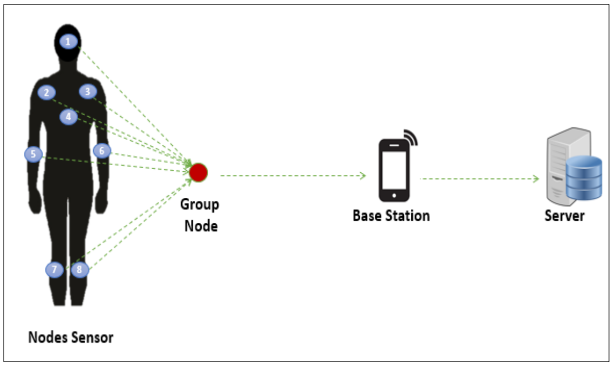
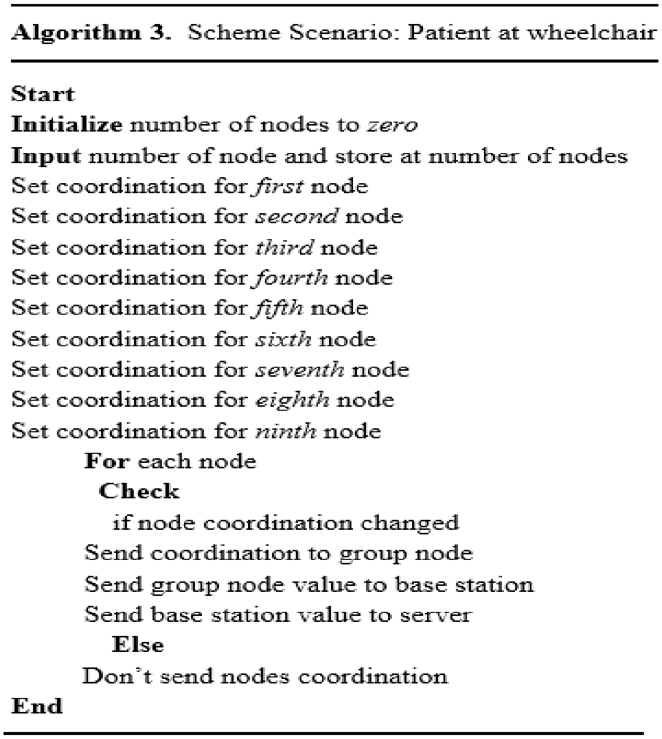


Fig 4. Scheme scenario: Patient at Bed

Scenarios 2: Patient in a Wheelchair. As shown in Figure. 5, we have a group node and eight sensor nodes which distributed around the patient's body (located in a wheelchair which moves between rooms) to gather general vital signs, such as Temperature, Blood pressure, Pulse, respiration and so on. These sensors nodes send gathered data to group node then group node forwards all data to Base Station then to the server. In this case; the patient will be in a Wheelchair and moves between rooms. So, the group node will follow the movement of the patient and based on that; both wearable sensors node and the group node will have full mobility. Algorithm 3. Shows scenario when patient in wheelchair "mobility status" and set eight sensors node around the patient body in different coordination, then send their values to group node then to the base station and finally to the server.



Algorithm 3. Scheme Scenario: Patient at wheelchair

```
Start
Initialize number of nodes to zero
Input number of node and store at number of nodes
Set coordination for first node
Set coordination for second node
Set coordination for third node
Set coordination for fourth node
Set coordination for fifth node
Set coordination for sixth node
Set coordination for seventh node
Set coordination for eighth node
Set coordination for ninth node
        For each node
          Check
            if node coordination changed
        Send coordination to group node
        Send group node value to base station
        Send base station value to server
            Else
        Don't send nodes coordination
End
```

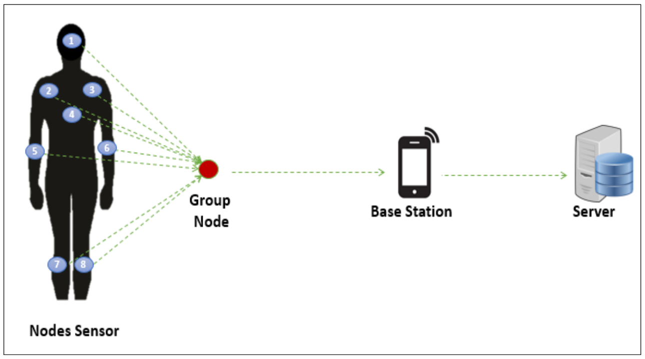


Fig 5. Scheme scenario: Patient at Wheelchair

4. Results Analysis

This section will offer analysis of consuming the energy of our proposed scheme. The analysis will include a comparison of the three cases: general scheme with no group node, our proposed scheme with a presence of group node, and Authenticated Key Agreement (AKA) protocol in both mobility and no mobility status.

This section offers a study and discussion of five different scenarios:

- No Group node without Mobility,
- No Group node with Limited Mobility,

- With Group Node without Mobility,
- With Group Node with Limited Mobility,
- Other study: Authenticated Key Agreement (AKA) protocol without Mobility,
- Other study: Authenticated Key Agreement (AKA) protocol with Mobility.

The analysis will focus and include a comparison between our proposed scheme with a presence of group node and with no group node scheme in both mobility and no mobility status. These scenarios are built and run at simulator (Contiki Cooja), then extract their results and compare consuming energy of each node and average energy for each scenario.

A. Case1. No group node without mobility

In this scenario, a patient lied on the bed, without applying the group node. This case was considered with 9 ultra-sensors nodes distributed on the patient's body for different vital signs. Normally, all ultra-sensors collect the required information and forward it to the base station and then to the healthcare server, as shown in figure 6, the scenario that built at simulation is without GN and mobility. The results based on this scenario are depicted in figure 7.

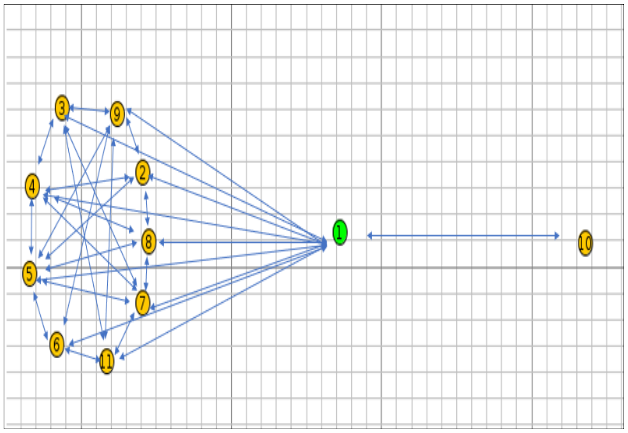


Fig 6. Simulator scenario of No group node – No Mobility

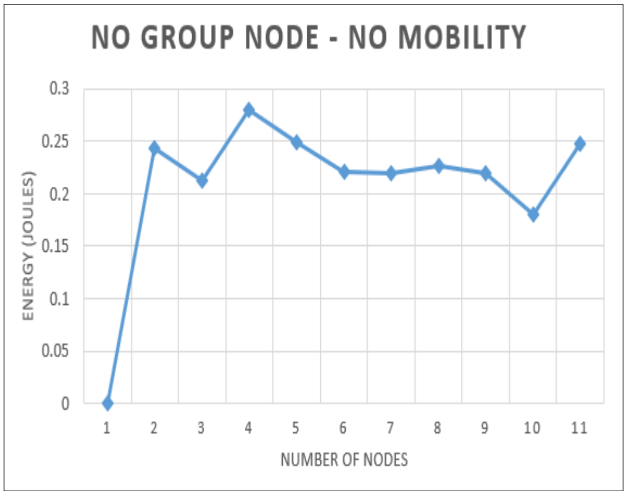


Fig 7. No group node – No Mobility

B. Case2. No group node with mobility

In this scenario, a patient sat on the wheelchair which can moves between the rooms, without applying the group node application. This case was considered with 9 ultra-sensors nodes distributed on the patient's body for different vital signs. Normally, all ultra-sensors collects the required information and forward it to the base station and then to the healthcare server, as shown in figure 8, the scenario that built at simulation is without GN but with mobility. The results based on this scenario are depicted in figure 9.

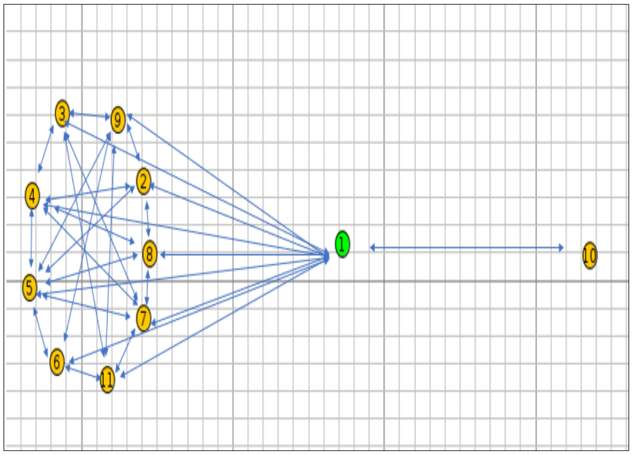


Fig 8. Simulator scenario of No group node – Mobility

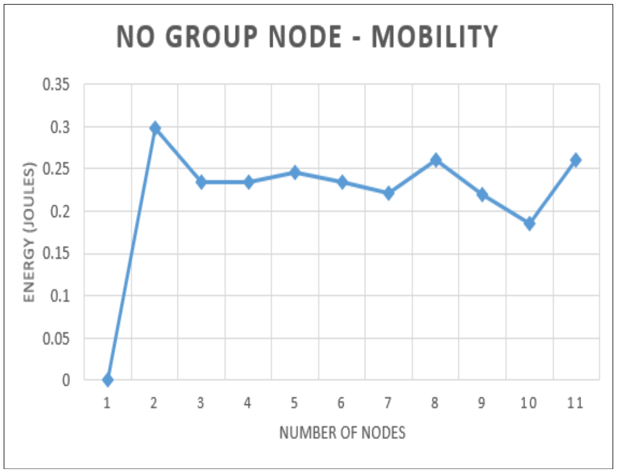


Fig 9. No group node –Mobility

C. Case3. With group node without mobility

In this scenario, a patient lied on the bed, in the presence of the group node, while 8 ultra-sensor nodes distributed on the patient's body for different vital signs other than the group node. Normally, all ultra-sensors collect the required information and forward it to group node then group node forwards all data to Base Station then to the server, as shown in figure 10, the scenario that built at simulation is with group node but without mobility case. The results based on this scenario are shown in figure 11.

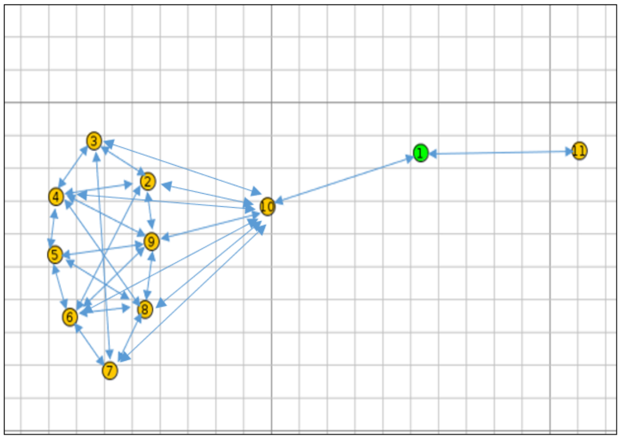


Fig 10. Simulator scenario of group node – No Mobility

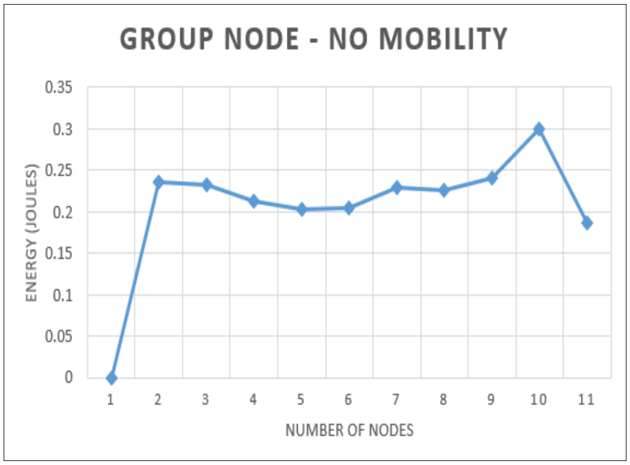


Fig 11. Group node – No Mobility

D. Case4. With group node with mobility

In this scenario, a patient is sat on a wheelchair, which can move between rooms, (as explained in section 3.5.2) with applying the group node application, and 8 ultra-sensors nodes were distributed to the patient's body for different vital signs. Normally, all ultra-sensors collects the required information and forward it to the group node then group node forwards all data to Base Station then to the server, as shown at figure 12 and explained for earlier cases. The scenario that was built at simulation is with group node, and with mobility. In this case; the group node will follow the movement of the patient and based on that; both wearable sensors nodes and the group node will have free mobility. The results based on stated scenario are presented in figure 13.

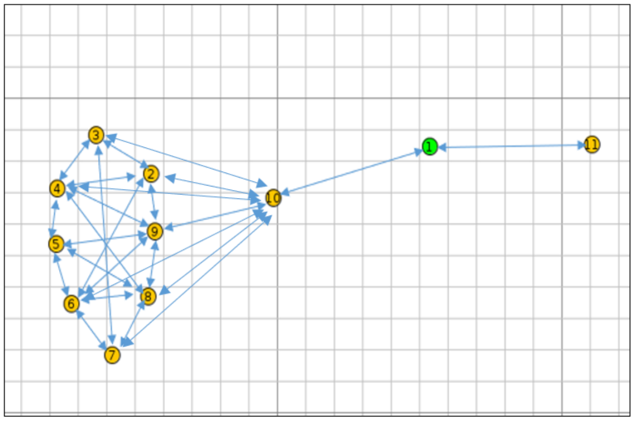


Fig 12. Simulator scenario of group node – Mobility

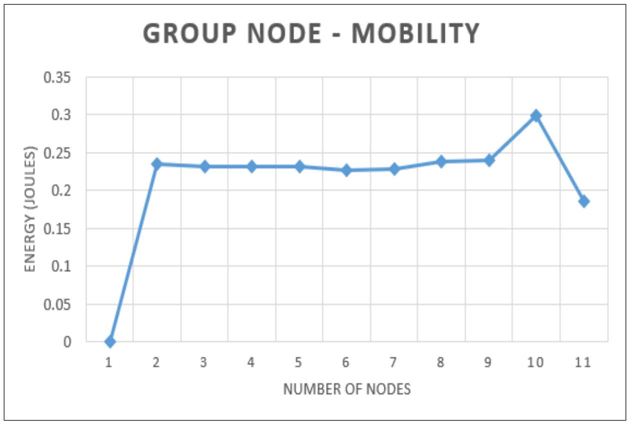


Fig 13. Group node –Mobility

E. Case5. Other studies: Authenticated Key Agreement (AKA) protocol without Mobility

In this study [17], they depicted a scenario which displays a number of several devices, including sensors, base stations and mobile device that communicate together to send and receive public/private key pairs {K pub, K priv}, as shown in figure 14, the scenario that built at simulation of AKA protocol case, that how it works. The results based on this scenario are shown in figure 15.

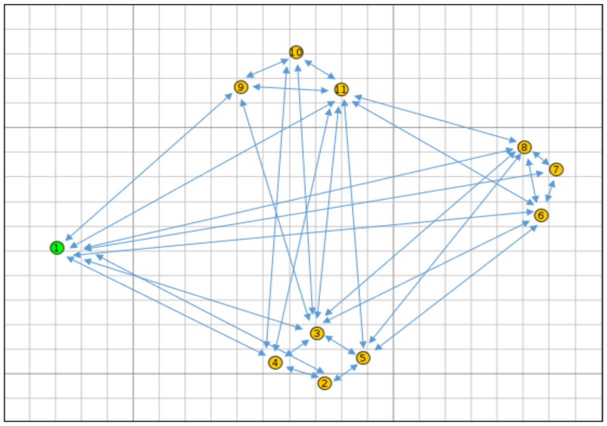


Fig 14. Simulator scenario of AKA

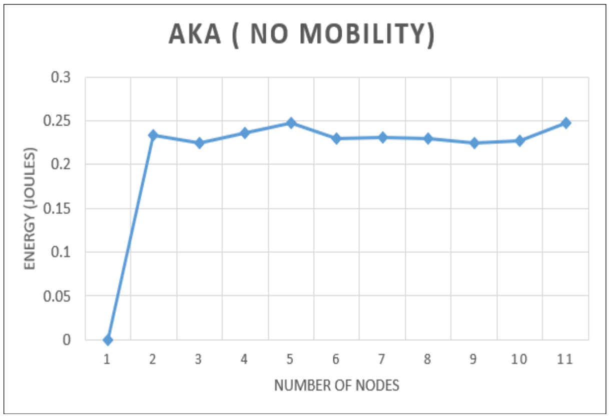


Fig 15. Energy results of AKA

F. Case6. Other study: Authenticated Key Agreement (AKA) protocol with Mobility

In the study[17], they depicted a scenario which display number of several devices, sensors, including base stations and mobile device that communicate together to send and receive public/private key pairs {K pub, K priv}, as shown in figure 16, the scenario that was built at simulator of AKA protocol case. The results based on this scenario are presented in figure 17.

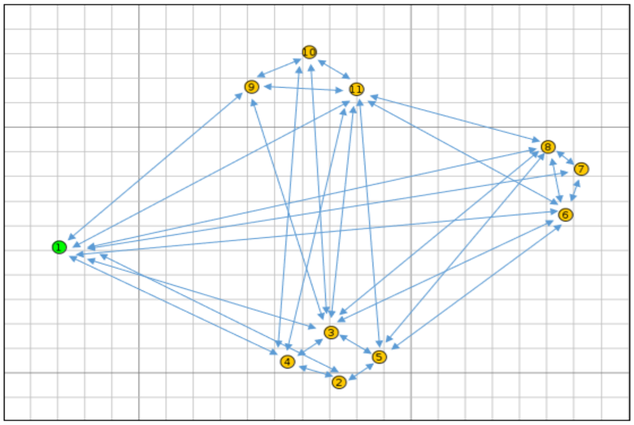


Fig 16. Simulator scenario of AKA

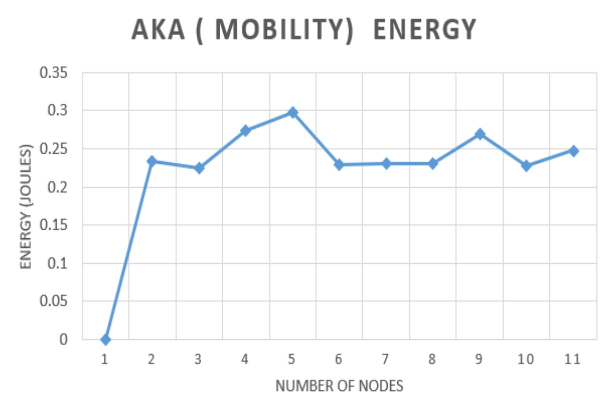


Fig 17. Energy results of AKA

5. Result Comparison

This subsection provides analysis of consuming the energy of our proposed scheme. The analysis includes a comparison among three cases: general scheme with no group node, our proposed scheme with the presence of a group node, and earlier work done, Authenticated Key Agreement (AKA) protocol.

5.1 General Scheme with No group node

As shown in figure 18, the general scheme without a group node. The results show that the energy consumption is higher in both of the cases, mobility and without mobility. In case, of direct data transfer from the ultra-sensory nodes to the base station. The energy consumption is higher, based on the distance from the nodes to the base stations. As the distance is directly proportional to the energy consumptions.

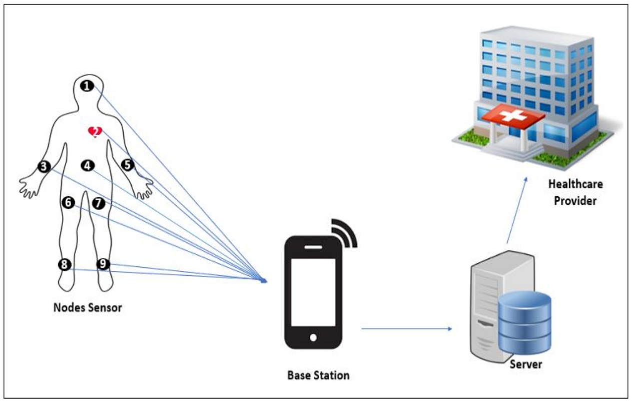


Fig 18. General Scheme with no group node

In addition, the energy is consumed higher due to the individual communication of each node with the base station to generate the authentication key, as of the case of 9 nodes. They are required to communicating at least 9 times to create receive the authentication key to transfer the data successfully. This multiple communication requires comparatively higher energy consumption as explained in figure 7 and figure 9.

5.2 Proposed Scheme with group node

In case, of the proposed scheme, as shown in Figure 19, where communication can be done at a shorter distance with the group node and this minimized the distance. Which leads to the less amount of energy can be used as it is significantly shown in figure 11 and figure 13. This also leads to more secure communication as all nodes may share one group-based authentication key scheme to handle all the same 9 ultra-sensor nodes. This reduces the chances of prone to the attacker compared to the earlier schemes.

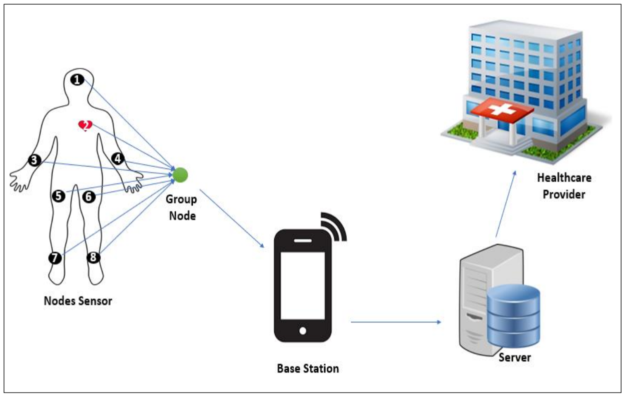


Fig 19. Proposed scheme with group node

We tested the same scenarios of the patient for both case of mobility, while a patient on the wheelchair and with non-mobility, while the patient is on the bed, using our proposed scheme where communication with the base station could be done by using the group node key concept. The Group Node (GN) key will share the common key among all ultra-sensor nodes and each node does not require communicating separately to get the authentication key for itself. This reduces the chances of the network to be prone to the attackers and this reduces the number of iterations of the network by n, which will have a direct impact on the energy consumption of the nodes.

The results show in figure 11 and 13, that the energy is optimized and less used compared to the case of non-group nodes and AKA protocol. The energy could be saved due to the shortening of communication distance and security could be higher by reducing the number of n number of iteration for getting the authentication key to transfer the data.

5.3 Authenticated Key Agreement (AKA) protocol

As shown in figure 20. Authenticated Key Agreement (AKA) protocol. The results show that energy consumption in both of the cases of mobility and without mobility; it is higher when different devices communicate together. The is because of the distance among the communicating nodes which is higher in the absence of the GN and as the distance is directly proportional to the energy consumptions, as explained in figure 15 and 17.

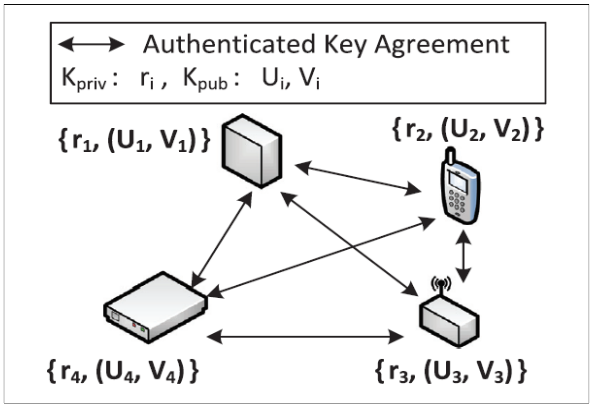


Fig 20. AKA protocol

Based on the achieved results for energy consumption for each node, which that represented in the graphs as depicted in previous scenarios. The average energy consumption for the different schemes. As depicted in the figure 21 and figure 22 for both of the cases of mobility and without mobility. The energy consumption is significantly lower with our proposed scheme, applying the group node. When we compare it with other schemes where no group node is applied for both of the cases either patient in the bed (no mobility) or the patient at the wheelchair (mobility) and (AKA) protocol. This significant change is due to the communication distances shorten in our proposed scheme based on GN.

Average energy is calculated based on the number of 9 nodes at each scheme. The average energy consumption is significantly lower in our proposed scheme with the group node when we compare it with others, as shown in table 1 and table 2.

Table 1: Average energy consumption for (No Mobility)

Average Energy (No mobility)	
No Group Node	0.23514
Group Node	0.23136
AKA	0.233028

Table 2. Average energy consumption for (Mobility)

Average Energy (Mobility)	
No Group Node	0.24562
Group Node	0.24062
AKA	0.246312

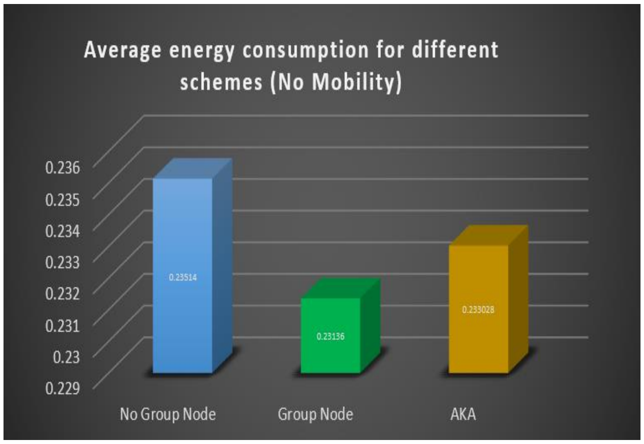


Fig 21. Average energy consumption for different schemes (No Mobility)

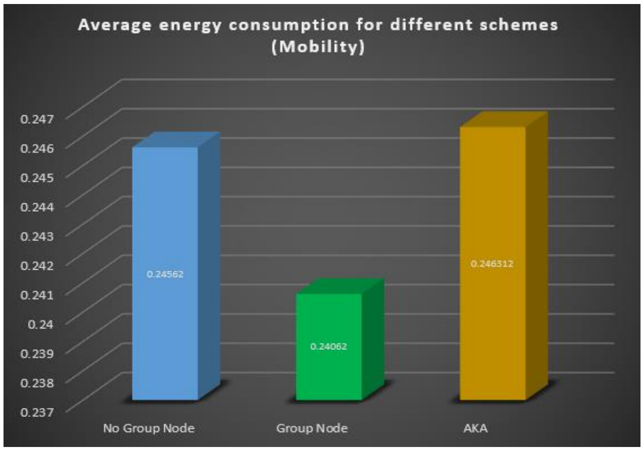


Fig 22. Average energy consumption for different schemes (Mobility)

Furthermore, the security is also higher in the case of a group node scheme. As under this scheme, the network will be exposed for a lesser time to the attackers, which will reduce the chances of possible attacks. This reduction of iterations for receiving the authentication by n number actually increases the security by n number.

6. Conclusion

This research introduces an efficient secured group-based lightweight authentication scheme for IoT based E-health applications. This scheme authenticates and establishes secure channels through sensor nodes and Base Station for E-health applications. This scheme differs from existing in a way that a Group Node (GN) concept has been introduced. The GN will issue the one common authentication key for the all nodes spread around the body of the patient and all nodes will share the one common key to communicate with themselves and to communicate with the base station and server using the GN as a leader. This scheme enhances the security level as well as the energy efficiency of the scheme. The (n) numbers increases the security, the same n number of communication iterations were reduced compared to existing techniques without GN concept, and this reduces the chances of the network to be prone for the attacker. At the same time, it increases the significant amount of energy by reducing the communication distance among the nodes, as we know that the communication distance has a direct impact on energy use. The proposed scheme was tested under different scenarios, such as involving mobility (patient on wheelchair) and non-mobility (patient on the bed) and the same cases with and without GN. Later these results achieved from the different scenarios, were also compared with existing popular schemes such as AKA and found a significant difference related to the energy efficiency and secure communication. Our scheme was evaluated using Contiki simulator. The achieved results, showed a significant difference in energy consumption and enhance the chances of security while receiving the authentication key. This all achieved by reducing the distance among the nodes and base station and as well as reducing the chances of external attacks by reducing the number of iterations by n for registering the authentication. Group-based node reduces distance and consumes less energy, as well as leads to reduce communication cost. In addition, it will be resistant against several types of attacks by using elliptic curve cryptography (ECC) techniques on the group-based node to increase the level of security in IoT based E-health applications.

References

[1] Khemissa, Hamza, and DjamelTandjaoui.“A Lightweight Authentication Scheme for E-Health Applications in the Context of IoT.” 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, doi:10.1109/ ngmast.2015.316

[2] Maksimović M., Vujović V. (2017) Internet of Things Based E-health Systems: Ideas, Expectations and Concerns. In: Khan S., Zomaya A., Abbas A. (eds) Handbook of Large-Scale Distributed Computing in Smart Healthcare. Scalable Computing and Communications. Springer, Cham

[3] Suhardi, and Alfian Ramadhan. “A Survey of Security Aspects for IoT in Healthcare.” Lecture Notes in Electrical Engineering Information Science and Applications (ICISA) 2016, 2016, pp. 1237–1247., doi:10.1007/978-981-10-0557-2_117 12

[4] Lee, J., Lin, W., & Huang, Y. (2014). A lightweight authentication protocol for Internet of Things. 2014 International Symposium on Next-Generation Electronics (ISNE). doi:10.1109/isne.2014.6839375

[5] Zeadally, S., Isaac, J.T. & Baig, Z. J Med Syst (2016) 40: 263. Retrieved from https://link.springer.com/article/10.1007%2Fs10916-016-0597-z at 29/09/2018

[6] Hossain, Md. Mahmud, et al. “Towards an Analysis of Security Issues, Challenges, and Open Problems in the IoT.” 2015 IEEE World Congress on Services, 2015, doi:10.1109/services.2015.12 3

[7] Williams, Patricia A H, and Vincent Mccauley. “Always connected: The security challenges of the healthcare IoT.” 2016 IEEE 3rd World Forum on IoT (WF-IoT), 2016, doi:10.1109/wf-iot.2016.7845455 2

[8] Anand, Sharath, and Sudhir K. Routray. “Issues and challenges in healthcare narrowband IoT.” 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), 2017, doi:10.1109/icicct.2017.7975247.

[9] Islam, S. M., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. (2015). The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 3, 678-708. doi:10.1109/access.2015.2437951

[10] Moharana, S. R., Jha, V. K., Satpathy, A., Addya, S. K., Turuk, A. K., & Majhi, B. (2017). Secure key-distribution in IoT cloud networks. 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS). doi:10.1109/ssps.2017.8071591

[11] Tarouco, Liane Margarida Rockenbach, et al. “IoT in healthcare: Interoperatibility and security issues.” 2012 IEEE International Conference on Communications (ICC), 2012, doi:10.1109/icc.2012.6364830

[12] Valera, Antonio J. Jara, et al. “An Architecture Based on IoT to Support Mobility and Security in Medical Environments.” 2010 7th IEEE Consumer Communications and Networking Conference, 2010, doi:10.1109/ccnc.2010.5421661

[13] Olga Boric-Lubecke, et al. “E-Healthcare: Remote monitoring, privacy, and security.” 10 July 2014. 10.1109/MWSYM.2014.6848602

[14] Berhanu, Yared, et al. “A testbed for adaptive security for IoT in eHealth.” Proceedings of the International Workshop on Adaptive Security -ASPI 13, 2013, doi:10.1145/2523501.2523506

[15] Suhardi, and Alfian Ramadhan. “A Survey of Security Aspects for IoT in Healthcare.” Lecture Notes in Electrical Engineering Information Science and Applications (ICISA) 2016, 2016, pp. 1237–1247., doi:10.1007/978-981-10-0557-2_11712

[16] Sangpetch, Orathai, and Akkarit Sangpetch. “Security Context Framework for Distributed Healthcare IoT Platform.” Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering IoT Technologies for HealthCare, 2016, pp. 71–76., doi:10.1007/978-3-319-51234-1_11

[17] Jr., Marcos A. Simplicio, et al. “Lightweight and escrow-Less authenticated key agreement for the IoT.” Computer Communications, vol. 98, 2017, pp. 43–51., doi:10.1016/j.comcom.2016.05.002 16

[18] T. Kothmayr, C. Schmitt, W. Hu, M. Br¨unig, and G. Carle, “Dtls based security and two-way authentication for the IoT,” Ad Hoc Networks, vol. 11, no. 8, pp. 2710–2723, 2013

[19] Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2017). A lightweight IoT security protocol. 2017 1st Cyber Security in Networking Conference (CSNet). doi:10.1109/csnet.2017.8242001

[20] Bala, D. Q., Maity, S., & Jena, S. K. (2017). A lightweight remote user authentication protocol for smart E-health networking environment. 2017 International Conference on

I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). doi:10.1109/i-smac.2017.8058330

[21] Fan, X., & Niu, B. (2017). Security of a new lightweight authentication and key agreement protocol for internet of things. 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN). doi:10.1109/iccsn.2017.8230088

[22] Patel, S., Patel, D. R., & Navik, A. P. (2016). Energy efficient integrated authentication and access control mechanisms for Internet of Things. 2016 International Conference on Internet of Things and Applications (IOTA). doi:10.1109/iota.2016.7562742

[23] Li, N., Liu, D., & Nepal, S. (2017). Lightweight Mutual Authentication for IoT and Its Applications. IEEE Transactions on Sustainable Computing, 2(4), 359-370. doi:10.1109/tsusc.2017.2716953

[24] Wu, X., Yang, E., & Wang, J. (2017). Lightweight security protocols for the Internet of Things. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). doi:10.1109/pimrc.2017.8292779

[25] Janbabaei, S., Gharaee, H., & Mohammadzadeh, N. (2016). Lightweight, anonymous and mutual authentication in IoT infrastructure. 2016 8th International Symposium on Telecommunications (IST). doi:10.1109/istel.2016.7881802

[26] Hussien, Z. A., Jin, H., Abduljabbar, Z. A., Hussain, M. A., Yassin, A. A., Abbdal, S. H., . . . Zou, D. (2016). Secure and efficient e-health scheme based on the Internet of Things. 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). doi:10.1109/icspcc.2016.7753621

[27] Goncalves, F., Macedo, J., Nicolau, M. J., & Santos, A. (2013). Security architecture for mobile e-health applications in medication control. 2013 21st International Conference on Software, Telecommunications and Computer Networks - (SoftCOM 2013). doi:10.1109/softcom.2013.6671901

[28] Fan, X., & Niu, B. (2017). Security of a new lightweight authentication and key agreement protocol for internet of things. 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN). doi:10.1109/iccsn.2017.8230088

[29] Park, Y., & Park, Y. (2017). A Selective Group Authentication Scheme for IoT-Based Medical Information System. Journal of Medical Systems, 41(4). doi:10.1007/s10916-017-0692-9

[30] Security in Building Automation Systems: a Study on Multi-party Key-agreement Protocols, Retrieve from www.politesi.polimi.it/bitstream/10589/102368/3/2014_12_Navoni.pdf. At 18/10/2018

[31] Maria Almulhim, Noor ZAMAN, “Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications” in 20th IEEE International Conference on Advance Communication Technology ICACT 2018, February 2018 Korea.

Ms. Maria Almulhim received the B.A. degree in Computer science from the College of Computer Science and Information Technology for girl in Hofuf, King Faisal University in 2012. Currently, study Master in computer science at the College of Computer Science and Information Technology, King Faisal University, Saudi Arabia. Current job, work as Programmer Analysis in National Guard and health affairs in Hofuf, Saudi Arabia. Her areas of interest include Software Engineering, Mobile Application Programming, Web Development, and Network Management.

Dr. Nazrul Islam Highly experienced and motivated Associate Professor of Computer Science with internationally proven track record (spanning 15 years) in research and lecturing (Bangladesh, Japan, UK, Italy, Estonia and currently Malaysia) with excellent academic promotion acumen and knowledge of Europe and South-East Asian academic and cultural expectations. Specialties: Robotics (Mobile and Industrial), Artificial Intelligence, Kinematics & Dynamics of Parallel Manipulators, Computational Mathematics and Soft Computing.

Professor. Noor Zaman acquired his degree in Engineering in 1998, and Master’s in Computer Sciences at the University of Agriculture at Faisalabad in 2000. His academic achievements further extended with PhD in Information Technology at University Technology Petronas (UTP) Malaysia. He has vast experience of 17 years in the field of teaching and research. He is currently working as A. Professor at College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia since 2008. He has contributed well in King Faisal University for achieving ABET Accreditation twice, by working as an active member and Coordinator for Accreditation and Quality cell for more than 09years. He takes care of versatile operations including teaching, research activities, leading ERP projects, IT consultancy and IT management. He headed the department of IT, and administered the prometric center in the ILMA University formerly Institute of Business and Technology (BIZTEK), in Karachi Pakistan. He has worked as a consultant for Network and Server Management remotely in Apex Canada USA base Software house and call center. Dr. Noor Zaman has authored several research papers in indexed journals\international conferences, and edited seven international reputed Computer Science area books, has many publications to his credit. He is an associate Editor, Regional Editor, Program Committee, Keynote Speaker and reviewer for reputed international journals and conferences around the world. He has completed several international research grants funded by different bodies and currently involved in different courtiers for research grants. His areas of interest include Wireless Sensor Network (WSN), Internet of Things IoT, Security, Mobile Application, Ad hoc Networks, Cloud Computing, Big Data, Mobile Computing, and Communication and Software Engineering.