Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 5517-5526*

Research Article

A Mutual Authentication Protocol for Telecare Services in an IoT Network

BakheNleya

Department of Electronic Engineering, Durban University of Technology, South Africa.(ORCID: 0000-0001-7252-2930)
bakhen@dut.ac.za

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: The emergence of Internet of Things (IoT), Cloud computing as well as the introducing of device to deice communication for devices in proximity has resulted in the emerging of new innovative services such as Tele-care in the health sector. However, issues such as privacy and security associated with such a service (Tele-care) are a challenge as most of the associated devices are resource constrained in terms of both operational power and computing capability requirements. As such it becomes problematic to implement any traditional as well as current privacy and security measures. Thus, in this paper, we mitigate on a framework to that will ensure a robust privacy as well as security for a Tele-care service. Notably our focus is in ensuring computational simplicity, privacy preservation as well as energy efficiency. Overall analysis shows that the proposed protocol has improved performance in comparison with existing ones.

Keywords: Tele-care, mutual authentication, D2D communication, privacy, security

1. Introduction

Telecare is an umbrella term for services and applications that aim to provision health services using the IoT as the main platform. For connectivity sake, the IoT is accessible via the GSM cellular network. Typical Tele care services and applications will include remote monitoring of patients, via networked dedicated sensors. In some cases, several of these sensors would be embedded within the body and interconnected via a Body Area Network (BAN). With the "advent of working from home" gaining momentum, Tele-care now extends to remote diagnosis as well as provisioning of health services to patients. D2D communication standards and protocols will facilitate medical devices interconnectivity in the realization of the various innovative Tele care related services and applications. Several otherwise catastrophic resulting medical conditions such as heart seizures (attacks) and high blood pressures can be closely monitored with complete privacy. In this regard the collaborative work on D2D Communication standards is ongoing under the umbrella of 3GPP by way of technical specifications and reports].

In parallel, lots of research is being carried out in order further enhance both privacy as well as general security Telecare based services and protocols. For instance, cloud server-based Tel-care services, applications and related authentication protocols are explored in [1], [2]. A symmetric cryptology-based authentication protocol is discussed in [3], whereas the studies in [4] mitigate a symmetric cryptology approach. Both studies seem to follow the same procedural steps, in ensuring that the authentication process and operation is similar and thus the following phases are defined: Initialization, Registration and Authentication. Physical security comparisons however reveal that the symmetric cryptology-based protocol is vulnerable as the patient's device is not completely secured from theft. At semantic level, the same protocol displays compromised confidentiality. Similarly, in [4] asymmetric and symmetric cryptography-based protocols that accomplish four phases of operation namely; hospital uploading (HUP), patient uploading (PUP), treatment and prescription (TP) and routing checkup (CP) are proposed. The authors assume the existence of a cloud server that will act as a storage of all retrievable medical related data mostly collected from sensors. Once again, some issues were identified pertaining to the security capabilities of both protocols. E.g. the protocol in [4], has physical security issues as the preservation of system anonymity cannot be guaranteed once the patient's devices is lost due to theft, neither is the same protocol immune Denial of Service (DoS) attack. In [5], [6] a hash Message Authentication Code (HMAC) based authentication protocols for D2Dcommunication are presented. The same study goes on to further extend the studies to developing an Identity-Based Signatures (IBS) version protocol. In [7] two group authentication protocols; one formulated around Identity-Based Encryption (IBE) and the other based on DHKE are investigated. In [8], the authors develop an optimized direct discovery model for the establishment of D2D communication links. In their formulation, they do make its functionalities be as similar as possible to the ProSec protocol standard developed by 3GPP. The authors in [9] presented an Elliptic Curve Discrete Logarithm Problem (ECDLP) based m-health authentication scheme for D2D communication. It is a certificate less encryption scheme (CLGSC) that protects ongoing sessions from eavesdropping . In this section, we analyze a

cryptography-based mutual authentication and key agreement protocol that whose candidacy for E-health is explored. In exploring the protocol, we focus on its resilience as well as abilities to provide security in terms of primitives outlined earlier such as resistance to attacks, confidentiality, and anonymity. We will also make a comparative performance analysis of this protocol in terms of computational complexity as well as communications overheads. The tendency to move towards energy efficiency networking prompts us to explore its efficiency in this regard as well.

2. Telecare Framework System

The system comprises patients, a hospital, cloud server as well as communication infrastructure. The communication infrastructure is enhanced with 3GPP access technology. Typical units which form part of the communication infrastructure include a Home Subscriber Server (HSS) typically housed in an evolved packet core (EPC), a few eNBs deployed in the coverage area as well as 3GPP [10],,[11]. New patients visit the nearest hospital for registration purposes. Their furnished information will be used for authentication purposes in future. E.g., authentication with the cloud server s mandatory before a patient's data can be uploaded or retrieved.

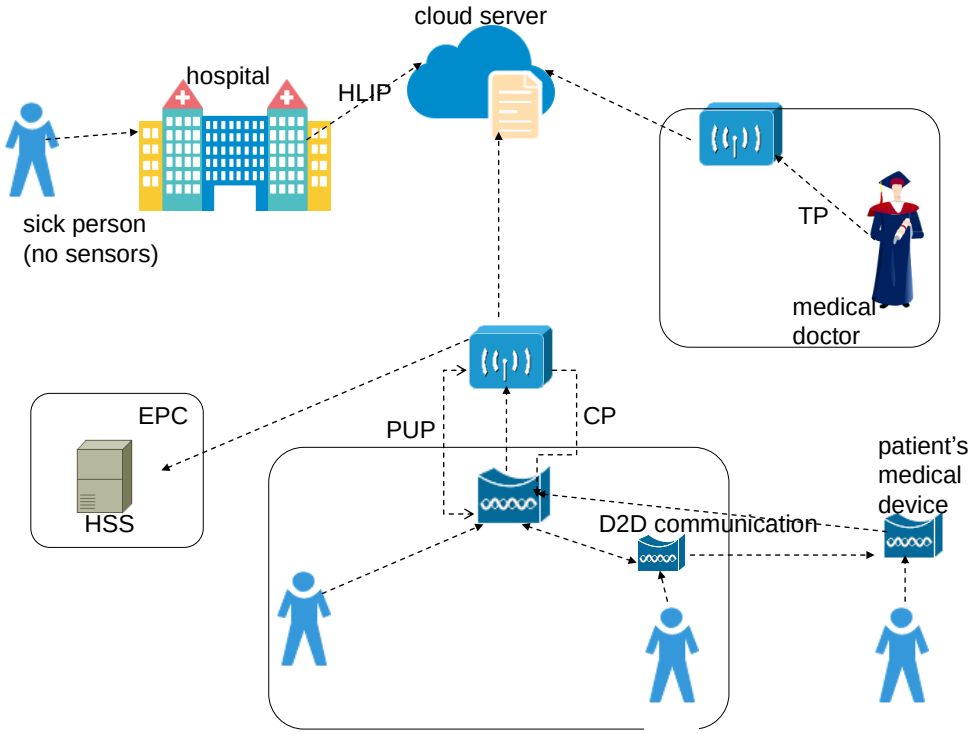

Figure.1. Tele-care system

Likewise, at devices level, each device performs a mandatory mutual authentication with the cloud server before any data exchange sessions can be sanctioned. Not all devices are within the 3GPP coverage infrastructure. Only those within its coverage may use it to access the cloud server. Otherwise, those which are not within coverage ranges rely on D2D communication to perform mutual authentication, prior to dispatching any patients related reports. Relays will also assist other D2D devices to reach the cloud servers. Devices that connect directly to the 3GPP infrastructure may also utilize D2D communication for data exchanges with the cloud and other key parties. The medical personnel, namely medical doctors are also expected to mutually authenticate before gaining access to a patient's records.

We next summarize the mandatory details of the multi-phase mutual authentication between the various entities (including patients and devices) and the cloud server as follows: used.

3. Related Work

The task of contention minimization in OBS switched backbone networks is accomplished by proper dimensioning of necessary and available resources at wavelength assignment, link and path levels. The key constraint being that more than one data burst cannot be assigned the same wavelength concurrently on the same link. At wavelength assignment level, various schemes such as random wavelength assignment, first-fit (FF),

minimum product, maximum sum, best-fit least loaded, least utilized, most frequently used and relative capacity loss have been explored [4]. The FF scheme generally performs relatively better in terms of burst loss probability and fairness. Furthermore, it has low computational overhead and complexity. To maximize on the number of simultaneous end-to-end lightpath connections, wavelength reassignment algorithms using minimum overlap and reconfiguration techniques have been suggested [5]. However, the suggested techniques only slightly reduce the blocking probabilities. The priority-based FF offline wavelength assignment scheme proposed in 6 is geared towards maximizing both the number of simultaneous connections as well as low burst losses. With this scheme, the wavelengths to be utilized for the connection requests are prioritized according to their estimated burst loss probabilities. The priority-based FF approach requires a longer setup time as it requires extra processing time to further estimate the loss probabilities on each selected lightpath connection.

At link and path levels, it is desirable that the shortest light path(s) from ingress to egress node be utilized, subject to constraints such as traffic load, congestion as well as wavelength assignment. As suggested in [7], efficient routing can be partly achieved by ensuring that path computation is optimized as much as possible. Examples include the Dijkstra algorithm-based routing protocols such as the O*pen Shortest Path First* (OSPF) and the *Intermediate System to Intermediate System* (ISIS). Whereas they always thrive to find an optimal path for each ingress to egress node pair, they however cause the same shortest links to become congested as well as be prone to contentions. With respect to the ingress-node destination pair, the longer paths remain underutilized and overall there is traffic imbalance in the network. In order to counter this, authors in [8] propose a distributed Path Computation Element (PCE) that enables routing protocols to efficiently utilize all available network links. PCE also applies software-defined networking (SDN) paradigms to separate signaling and routing paths, thus giving more network control to operators and in that way, contentions are reduced overall. An algorithm called the Self-Tuned Adaptive Routing (STAR) [9], was further incorporated to enhance traffic balancing as well prevent links from being overwhelmed.

A dynamic contention as well as congestion aware scheme that seeks to reduce blocking probabilities as well as boosting utilization by symmetrically distributing network traffic over all active links was proposed in [10]. Finally, in [11], the researchers proposed and investigated a per-link congestion control-based scheme that seeks to balance available network resources allocation by utilizing present and forecast demands of lightpath requests statistics. In essence, practical networks have a regularized topology and lightpath connection requests are generally random in nature. Given a fixed amount of resources (link, wavelengths, paths, as well as constraints), an increase in the traffic load results in the reduction of the number of idle resources per link and hence this will lead to both contention as well as blockings.

4. Proposed Authentication Protocol

We now proceed to describe, discuss as well as analyze the Group Authentication scheme in a D2D Communication based telecare framework which among other things will involve as well as enable large volumes of confidential health related data It was proposed in [6] and it is symmetric cryptography based. Fig 1.in section II is provided to illustrate the system overall.

We next summarize the mandatory details of the multi-phase mutual authentication between the various entities (including patients and devices) and the cloud server as follows: used.

4.1 Device Discovery Scheme

For the invoking of any service, which might include several devices, each of the group members must perform neighbor device discovery to identify collaborating devices within vicinity. Each device does that via the HSS. The Home Subscriber Server (HSS) will in turn verify whether its International Mobile Subscriber Identity (*IMSI*) matches the device records in its database and whether the device is indeed authorized (privileged) for the intended service, plus it is D2D communication compliant. Upon successful verification, the authorization will be relayed to eNB and at the same time tagged with a timer.

Next, all verified devices belonging to a group can now mutually identify each other as belonging to that group by possibly using WLAN direct radio signals is sharing their attributes.

4.2 Registration Phase

Key mutual authentication-related primitives are exchanged during this phase, The IMSI of each device must be registered in the HSS and normally this is done by the vendor. All key personnel and patients are registered to the cloud server via some identified secured channel. Each device is assigned a temporary identity.

$$TID_y = h_1(ID_y \| R_k) \tag{1}$$

where R_k is an arbitrary chosen random number that will remain mapped to their real identities ID_y; h_1 is a hash function for the TID_y generation.

Both the real and temporary IDs will be furnished to the cloud server for storage and subsequent use in other authentication phases.

4.3 Hospital Uploading Phase (HUP)

This phase is exclusive to registered entities. At this stage, preparations are being made to mutually authenticate parties that will be involved in the updating of any data acquired from the patient. The authentication does not necessarily need to be done on a secured channel. Rather an unsecured channel is preferred for the purpose. The phase commences with the would be patient (user) paying a visit to his/her nearest health center for a health checkup. Alternatively, this could be due to some evident ailment. At the health center the patient will be issued with login credentials which can now be used to access the service via a standard GSM handset (smart phone). The overall authentication at this phase is sequentially carried out as follows:

Using a randomly generated integer R_h and its real identity ID_h the hospital computes its own message authentication code (MAC_h) as follows:

$$MAC_{hs} \rightarrow h_2(|ID_h|)(R_h) \tag{2}$$

Where, h_2 is a has function for generating the MAC. Later, the key primitives are relayed to the cloud server in the form of a time stamped (T_h), message (m_1);

$$m_1 \rightarrow (TID_h, R_h, MAC_{hs}) \tag{3}$$

Upon receiving m_1 together with T_h from the Hospital the cloud server performs the necessary validations by initially computing:

$$MAC_{hs}' \rightarrow' h_2(ID_h // R_h) \tag{4}$$

Note that the validation of (4) above is done using the real and temporary identities furnished by the hospital at registration phase. It therefore suffices to compares its own computed MAC and that contained in m_1

$$MAC_{hs}' \rightarrow MAC_{hs} \tag{5}$$

Upon successful authentication, it goes on to select a random number R_{sh} before computing.

$$MAC_{sh} = h_2(ID_h // R_{sh}) \tag{6}$$

This will now be sent as a time stamped (T_s) confirmation message (m_2) back to the hospital.

$$\mathrm{m2} \rightarrow (MAC_{sh}, R_{sh}) \tag{7}$$

Upon receiving the time stamped message m_2 from the server, likewise the hospital performs all the necessary validations as follows:

First, it checks that the validity of the received time stamp. This is followed by re-computing of the following.

$$MAC_{sh}' \rightarrow' h_2(ID_h // R_h) \tag{8}$$

After which it verifies that the two MACs match.

$$MAC_{sh}' \rightarrow MAC_{sh} \tag{9}$$

Subject to the validity of (9), the next step would be to generate a common session key.

$$K_{hs} = h_3(ID_h // R_{h// R_{sh}}) \tag{10}$$

Where h_3 once again is a MAC generation function; R_{sh} is a randomly generated number by the cloud and sent to the hospital. A session key validator is also computed, with the help of a session key generator hash function h_4 as follows:

$$C_{hs} = h_4(K_{hs}) \tag{11}$$

The session key is used to cipher the patient's records before uploading to the server in the form of a message $m_3 = M_{rp}$;

$$M_{rp} \rightarrow E_{K_{hs}}(patient\ record, TID_h, C_{hs}) \tag{12}$$

The message m_3 is then time stamped from the hospital side before dispatching it to the cloud server.

Upon receipt of m_3 and T_h the cloud server computes the session key

$$K_{hs} \rightarrow h_3(ID_h // R_h // R_{sh}) \tag{13}$$

and deciphers the patient's report.

$$(patient's\ record, TID_R, C_{hs}) \rightarrow D_{K_{hs}} \tag{14}$$

Ultimately it computes, $C_{hs} = h_4(K_{hs})$ and validates:

$$C_{hs}' = C_{hs} \tag{15}$$

Only then will the records be admitted to the Cloud server's database.

4.3 Patient Uploading Phase (PUP)

This involves uploading all acquired patient's health related data via sensors to be uploaded to the cloud server. This can be done over a generally insecure channel since most patients are scattered around the countryside and with not sufficient network (3GGPP)/ coverage. This data will thus be encrypted for confidentiality sake. The patient's main device will prompt all sensors within vicinity (around his/her body) to release the data to it. Authentication is necessary before the data collection by the main patient's device initiates. It is important to note that all associated devices must be initially successfully authenticate with the available 3GPP network.

If they are to utilize the D2D communication mode, then a random number R_p, is generated by the patient's device. It uses this same number to compute a hash of its $IMSI$.

$$Auth_p = h_1(IMSI_p \| R_p) \tag{16}$$

Ultimately the hash is sent to the HSS for use in the authentication verification according to:

$$Auth_p^{'} = hi(IMSI_p \| R_p) = Auth_p \tag{17}$$

Once authenticated by the HSS the patient's device can perform discovery with peer proximity devices using their temporary devices as well. It is also possible for a device that is outside a 3GPP coverage area to rely on close by devices to access the 3GPP network coverage range and ultimately authenticate with the cloud server.

4.4 Prescriptions Phase (PP)

Once again the two parties involved; the medical specialist and cloud server must mutually authenticate. Ultimately a session key will be generated and used to cipher all patients reports, body sensor measurements as well as the overall diagnosis. The procedures taken are as follows.

The medical specialist must initiate the authentication with the server by generating a random number R_d as well as providing a temporary ID (TID_d). The two will be used to generate:

$$MAC_{ds} = h_2(ID_d // R_d) \tag{18}$$

Which is now time stamped (T_d) and dispatched to the server in the form of a message m_1.

$$m_1 = (TID_d, R_d, MAC_{ds}) \tag{19}$$

Upon receiving both m_1 and T_d the server validates them before further computing $MAC_{ds}' = h_2(ID_d // R_d)$ and ultimately verifying $MAC_{ds}' = MAC_{ds}$.

Should the verification succeed, the server once again opts a random integer R_{sd} and uses it to compute the MAC and session key:

$$MAC_{sd} = h_2(ID_d // R_{sd}) \tag{20}$$

$$K_{ds} = h_3(ID_d // R_d // R_{sd}) \tag{21}$$

$$C_{ds} = h_4(K_{ds}) \tag{22}$$

The server uses the session keys to cipher the patients records it retrieves from the data base:

$$M_{RpMS} = E_{KHC}(p\_RR, sensor, TID_p C_{ds}) \tag{23}$$

Finally it time stamps (T_s) the records and sends them in the form of a message m_2 to the medical specialist.

$$m_2 = (MAC_{sd}, R_{sd}, M_{RpMS}) \tag{24}$$

Upon receiving m_2 and T_s , the medical specialist validates them and ultimately generates a session key:

$$K_{ds} = h_3(ID_d // R_d // R_{sd}) \tag{25}$$

He will then decipher the received patient records before sending a time stamped confirmation message (m_3) back to the cloud server. The latter will have to positively validate m_3 otherwise this a malicious activity of the side of the medical specialist (i.e., a hacker is attempting to infiltrate the system).

5. Performance Analysis

In this section we summarily analyze the protocol in terms of security requirements as well as performance. The performance is restricted to computational simplicity, communications overhead as well as energy efficiency.

5.1 Security Analysis

Mutual Authentication: With the protocol any two communicating parties reciprocate each other in computing the MAC for mutual authentication purposes.

Forward/Backward Secrecy: The protocol relies on the generation of random values in each initiated session hence the old system keys are not valid for future sessions. In that way backward secrecy is guaranteed. Similarly, keys intended for future use are not valid for use in already past sessions, and thus it is for that reason that forward secrecy is guaranteed.

Confidentiality: The protocol runs authentication scripts for very session. Specifically, each session key generation is robustly authenticated.

Non-Repudiation: The use of temporary identities by all parties (TIDH, TIDP, TIDD) and restricting the knowledge of real identities to the cloud server ensures non-repudiation.

Anonymity: Assigning and relying on temporary identities (TIDH, TIDP, TIDD), for authentication purposes ensured anonymity. The cloud server is secluded in the authentication process hence the reliance on insecure channels for the initial authentication does not compromise its identity.

Non-Traceability: Periodically changing temporary identities or assigning a set to each entity ensures non traceability. This is further enhanced with the use of randomly generated numbers for each authentication procedure (session)

Session Key Security: Session keys are localized and not exchanged. In that way they cannot be intercepted along compromised channels in case they were exchanged via such channels.

Impersonation Attack: The lack of knowledge of real identities of both the cloud server and the rest of the entities means intruders or attackers have no chance in succeeding to impersonate them. Furthermore, a valid MAC is a function of the associated entity's real identity.

Replay Attack: Random values are constantly generated for computing new session keys and other authentication related primitives hence this secludes the possibility of an attacker succeeding to forge messages utilizing old values.

Denial of Service (DoS): Usage of time stamping throughout secludes the possibility of DoS attacks,

Man-in-the-Middle Attack: Authentication is accomplished using exchangeable values and localized(un-exchangeable) values. In that way Main-in-the –Middle attacks are impossible to execute

5.2 Performance Analysis

In this subsection, we analyse the performance of the protocol. In this regard we carry out a comparative performance analysis of the computational demands (intensities), communication overheads as well as energy efficiencies [14], [15] of the proposed versus similar protocols presented in [6] and [12].

The evaluation of computational costs of the protocols are solely based on an estimate of the time lapses required to accommodate the execution of operations, that are regarded as integral part of the messages exchanged in the various phases of each protocol. Provided in Table 1 are example operations and associated computational costs of the proposed protocol.

Table 1. Various operations execution times (normalized)

symbol	*defination*	$\cos t(\sec s)$
T_p	pairing	0.061
Ts	signature	0.06
T_E	ciphering/deciphering	0.0087
T_H	one way hash operation	0.005

For the proposed scheme, the total computational load will be the aggregated from the 4 phases described in the preceding section.

$$C_{total} = 12nT_E + 30nT_H \equiv 0.051n \tag{26}$$

For [6], the total computational load is given by:

$$C_{total} = 4nT_s + 9nT_E + 35T_H = 0.021n \tag{27}$$

For [12] we have.

$$C_{total} = 5nT_s + 11nT_p + 8nT_E + 32nT_H \tag{28}$$

We now compare the computational loads of the three schemes namely the proposed, and two others proposed in [6] and [12] respectively. The number of devices per group, or rather in a particular target area is varied from 0 to 100.

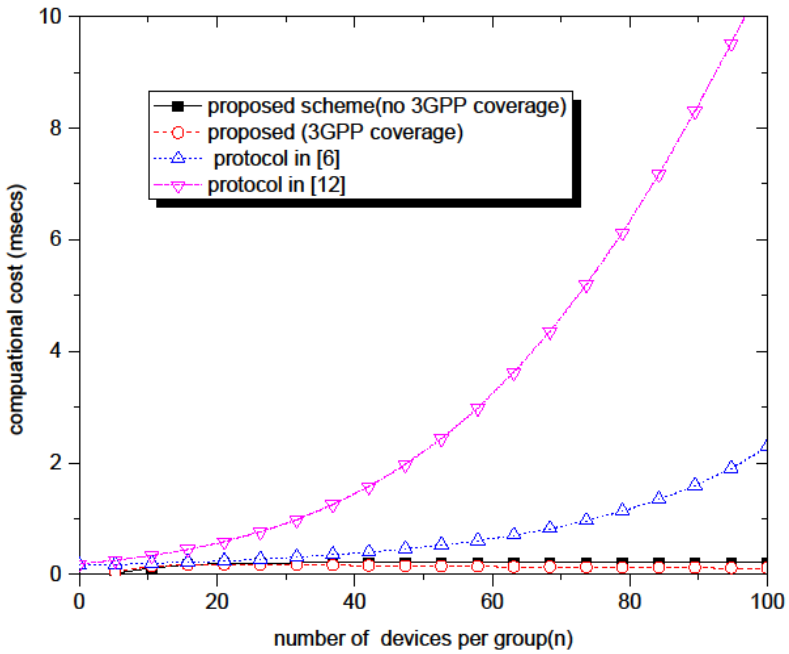

Fig.2. Computational cost comparisons

Figure 2 plots the relative computational costs in which we see that the proposed requires the lowest computational cost.

With regards to communication overheads comparison, it is noted that in general, D2D communication cost metrics are depended on the volumes of exchanged signaling data over insecure channels. The communication cost and required transmission bandwidth are directly proportional. Associated parameters corresponding costs are shown in the table below.

Table 2. Communication costs

action	overhead
Time stamping, random integer , TID	6 bytes
Hash function/ pairing	2. bytes
Session key	16 bytes
Signature	64 bytes

The total overheads in bytes required by each scheme are as follows:

For the proposed scheme.

$$comm_{total} = 384n + 66m - 26 \tag{29}$$

where, n is the number of active devices and m would be the number of messages exchanged.

The protocols proposed in [6] and [12] will correspondingly require $384n$ and $865n$, bytes overhead respectively.

Plots of the communication overheads for the three protocols as a function of the number of active devices is provided in figure 3. From the same graph, it can be deduced that the proposed protocol generates relatively low communication overheads hence it is best suited for adaptation to D2D communication.

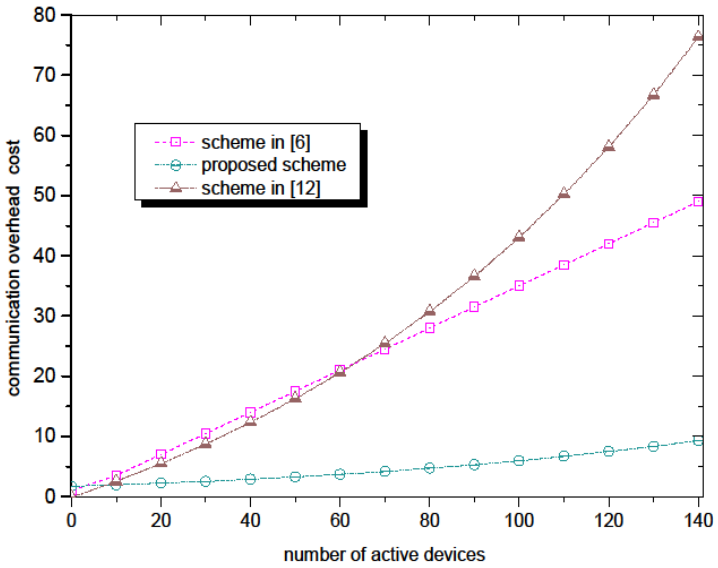

Figure.3. Communication cost comparisons

The other two schemes incur relatively much higher communication overheads s, since they involve the exchanging of quite a few costly signature parameters, for their mutual authentication. As we gradually move towards energy efficient aware networking and protocol design, [15], [17]. It is necessary to minimise on the operational energy requirements of any protocol thereof. Besides most of the devices are resource constrained in terms of power supply. Most of the energy consumptions are incurred by the CPUs of the respective devices.

The normalized energy cost for the various protocols are calculated as set out in the next three following formulae:

For the proposed protocol:

$$E_{total} = 12nT_E + 33nT_H \tag{30}$$

For [6]

$$E_{total} = 4nT_s + 9nT_E + 35nT_H \tag{31}$$

For [12]

$$E_{total} = 5nT_s + 11nT_p + 8nT_E + 32nT_H \quad (32)$$

A plot of the operational energy requirements for the 3 different schemes is provided in Fig 4.

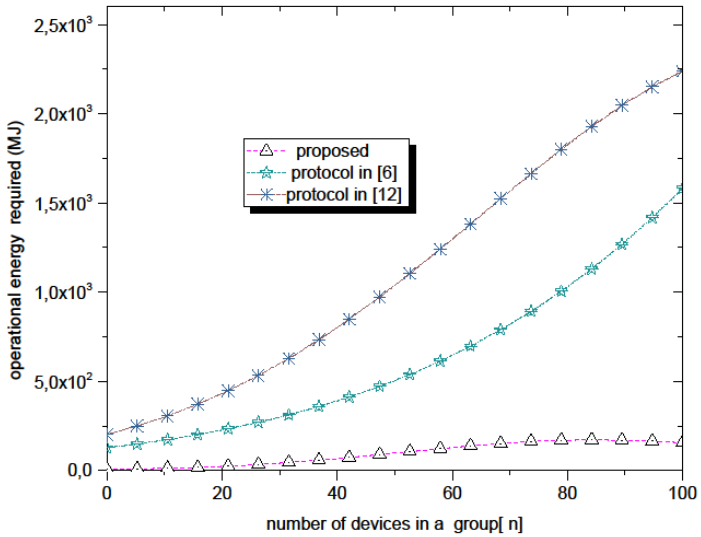

Figure. 4. Energy cost comparison

By comparison, proposed scheme in is more energy efficient.

6. Conclusion

This paper proposes a D2D communication-based authentication and key agreement Tele-care scheme that ensures both privacy and security for patients who have enrolled for the service. The fact that the authentication can be done via an insecure link means that even in the absence of 3GPP network coverage, patients would still be able to link with the nearest health care center and medical specialists, thus making the scheme both resilient and robust. This is because D2D communication supports direct device linking of proximity devices and thus an affected device would still reach the nearest peer that is within sufficient coverage range.

The paper uses lightweight message authentication that is meant to reduce computational and communication loads, as well as operating in an energy efficient manner. Its efficacy in terms of ensuring both security and privacy was explored. Overall, we conclude that the scheme would be quite viable in the practical implementation of telecare as most of the devices are resource constrained in terms of computational as well as operation power requirements.

References

L. Bopape, B. Nleya, A. Mutsvangwa, P. Khumalo, “A Group Authentication And Data Security Scheme For Smart Metering In Smart Grids”, Ponte - Jan 2020 - Volume 76 - Issue 1, doi: 10.21506/j.ponte.2020.1.4

M. A. Kamoona and A. M. Altamimi, "Cloud E-health Systems: A Survey on Security Challenges and Solutions," 2018 8th International Conference on Computer Science and Information Technology (CSIT), Amman, Jordan, 2018, pp. 189-194, doi: 10.1109/CSIT.2018.8486167.

I. Erguler and E. Anarim, "A Password-Based Key Establishment Protocol with Symmetric Key Cryptography," 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Avignon, France, 2008, pp. 543-548, doi: 10.1109/WiMob.2008.112.

C. de Canniere, A. Biryukov and B. Preneel, "An introduction to Block Cipher Cryptanalysis," in Proceedings of the IEEE, vol. 94, no. 2, pp. 346-356, Feb. 2006, doi: 10.1109/JPROC.2005.862300.

A. Paula G. Lopes and Paulo R. L. Gondim , “Mutual Authentication Protocol for D2D Communications in a Cloud-Based E-Health System”, Sensors, April, 2020, doi:10.3390/s20072072

M, Wang, and Z., Yan, “Privacy-preserving authentication and key agreement protocols for D2D group communications”, IEEE Transactions on Industrial Informatics, vol.14, no.8, pp.3637-3647, 2018.

R. H., Hsu, J., Lee, T. Q., Quek, and J. C., Chen, “GRAAD: Group Anonymous and Accountable D2D Communication in Mobile Net-works.”, IEEE Transactions on Information Forensics and Security, vol.13, no.2, pp.449-464, 2018.

A. Nauman, M. A. Jamshed, Y. Ahmad, R. Ali, Y. B. Zikria and S. Won Kim, "An Intelligent Deterministic D2D Communication in Nar-row-band Internet of Things," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 2019, pp. 2111-2115, doi: 10.1109/IWCMC.2019.8766786.

P. Kushwaha, "Towards the equivalence of Diffie-Hellman problem and discrete logarithm problem for important elliptic curves used in practice," 2017 ISEA Asia Security and Privacy (ISEASP), Surat, 2017, pp. 1-4, doi: 10.1109/ISEASP.2017.7976981.

M. Gomba and B..Nleya, "Architecture and security considerations for Internet of Things," 2017 Global Wireless Summit (GWS), Cape Town, 2017, pp. 252-256, doi: 10.1109/GWS.2017.8300477.

L. P. Bopape, B. Nleya and P. Khumalo, "A Privacy and Security Preservation Framework for D2D Communication Based Smart Grid Ser-vices," 2020 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2020, pp. 1-6, doi: 10.1109/ICTAS47918.2020.233995.

L. Chiou, S., Ying, Z. and Liu, J., "Improvement of a privacy authentication scheme based on cloud for medical environment”, Journal of medical systems, v. 40, n. 4, pp.101, 2016.

Mohit, P., Amin, R., Karati, A., Biswas, G. P., Khan, M. K., "A standard mutual authentication protocol for cloud computing-based Health care system.", Journal of medical systems, v.41, n. 4, pp. 50, 2017.

B. Nleya and C. Mulangu, "An Overview of GREEN Networking and Power Savings in Optical Backbone Networks," 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 2018, pp. 1-6, doi: 10.1109/ICABCD.2018.8465402.

B. Nleyaand R. Chidzonga, "Overview of power aware — RWA in optical backbone supported networks," 2017 IEEE AFRICON, Cape Town, 2017, pp. 446-449, doi: 10.1109/AFRCON.2017.8095523.