ISSN 2278-3091
Volume 8, No.3, May - June 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse58832019.pdf
https://doi.org/10.30534/ijatcse/2019/58832019

Lightweight Security Protocols for Internet of Things: A Review

Deepti Rani, Nasib Singh Gill
Department of Computer Science & Applications
Maharshi Dayanand University, Rohtak, Haryana (India)
deepti.sindhu@gmail.com, nasibsgill@gmail.com

ABSTRACT

Smart devices and IoT applications have been widely used in many fields of social living, social production, home and industrial automation which have made people's life efficient and convenient. But in recent years, ubiquitous deployment of some tools and technologies has raised several concerns related to the privacy and security in IoT enabled smart environment. The present paper presents a range of various existing as well as proposed lightweight security protocols. Security protocols are designed to make secure communication within IoT enabled environment with less computation and storage cost. Lightweight protocols are characterized by relatively small overhead. The paper also presents a comparative study of various lightweight security protocols for IoT, proposed by many researchers in recent years. Lightweight cryptography algorithms used for designing lightweight security protocols have also been explored in present paper.

Key words: IoT, Security in IoT environment, Lightweight Protocols, Security Protocols, Lightweight Cryptography Algorithms, Cryptographic Techniques, Comparative Analysis of Protocols.

1. INTRODUCTION

IoT has been utilized in various application domains like smart homes, smart industries, smart cars and etc. Users receive IoT services by connecting to multiple servers over various kinds of networks which can bring to IoT systems a plethora of serious security and privacy risks. The main causes of these attacks are hardware and software vulnerabilities. Mirai botnet and Ransom-ware are the most prominent instances of security attacks. Privacy risks are created for the consumers associated with collection of sensitive and personal information in IoT environment [1]. Secure authentication solutions are mandatory for user's systems [2]. Some existing solutions are very expensive. Hence secure, lightweight and well scaled protocols were needed with low cost tags [3]. But most recently proposed work of many researchers is focusing on extremely lightweight security protocols.

The term Internet of Things (IoT) was first proposed during 1999 by Kevin Ashton in MIT Auto-ID center. In 2005, ITU revised IoT with four main technologies using which IoT is attaining great attention of users [4]. These technologies are RFID technology, nano technology, wireless sensor-technology and intelligent system. But many scientific literatures have discussed about this concept earlier to this proposal. Everyday a number of devices are being connected to one or many devices globally and many additional smart devices are being added to smart Internet world. People are now frequently joining smart IoT world using these devices. Maximum of these devices generally include constrained devices including smart handheld devices (smart mobile phones), smart home equipments, transportations and other smart electronic user controlled devices [5]. Constrained devices are limited by storage capacity, energy consumption and computing. These devices are connected via Internet or cloud and are managed in wireless sensor networks. Each of these devices has a unique identification number that can be an IP address or any other unique ID code [6]. Protocol stacks and related software are necessary part of realization of IoT devices in existing network. Protocols are also helpful in communicating these devices to other devices [7].

2. SECURITY IN IOT ENVIRONMENT

Although IoT devices have made human life very easy and comfortable but they also keep people's personal information at risk. Information could be hacked from user's personal storage devices which are connected to Internet. Today, security is the major concern. Therefore, IoT devices and software to be used on these devices must be provided with security.

Security is the main concern in networking system due to weak security mechanism. Each device containing an IP address connected to a network must be authenticated in order to protect against certain types of attacks. It is also important that protocols to be used while communication also need to meet security requirements [8]. Communicated data also need to be encrypted and authenticated [9]. Various communication technologies are used for communication, some of which are Wi-Fi, Wi-Max, Wi-Mi, BLE, Satellite, DASH7 (RFID) and many other remote technologies which have their own communicating range [6] [10]. An IoT environment must be enriched with following features [11]:

- Constrained
- Diversity
- Mobility
- Myriad
- Intimacy
- Unattended
- Ubiquitous
- Interdependence and etc.

Security Protocols: Privacy and security are very important aspects for IoT based application domains. To understand security protocols better, one needs to study and understand some mandatory and updated security features [12]:

- Confidentiality
- Privacy
- Integrity
- Interdependence
- Diversity
- Secure Routing
- Robustness
- Resilience
- Attack Detection

Lightweight Protocols: Heavy weight algorithms are not much suitable for the security of IoT. Therefore, Lightweight security algorithms were introduced as alternative solution for security of IoT [13].

Lightweight protocols refer to those protocols which are used for transmission over a network with lesser overhead. These protocols are lesser in size, faster, simpler and easier to manage many other communication protocols. Code of lightweight protocols performs faster than other standard protocols. Lightweight protocols generally use data compression techniques to get lighter effect.

Discovery and Registration: Discovery of available nodes (devices) is important part of a protocol. DISCOVERY is a method that is used to make a scan network via Wi-Fi, Bluetooth, LAN and Ethernet. But this method is not applicable for discovering IP based communication. Only the devices with IP address can communicate in a network.

Security Algorithms: Privacy and Security are indispensable elements which are required to be addressed to retain the faith of IoT users. Current security solutions used at each layer are vulnerable to variety of attacks. This section provides an overview of some existing lightweight security algorithms used for the security of IoT environment [13].

Lightweight Cryptography: Large numbers of smart devices can be connected to the Internet and all these devices can interact with each other. But these devices might be attacked and accessed by unauthorized users. It is not easy to implement cryptography on each connected device individually. Devices connected to IoT have low bandwidth, limited frequency, low power and storage capability.

Lightweight cryptography is popularly implemented in IoT enabled smart environments for data security. Authors in [13] discussed various lightweight security algorithms. Yao et al. in [14] proposed an improved algorithm with reduced communication and computational overhead. Efficiency of algorithm has been improved using ECDH algorithm. Different modules have been designed to implement the encryption algorithm. In [15] it has been implemented with LPWAN and LoRaWAN network technologies.

LWC Algorithm: Lightweight cryptography algorithm was introduced to fulfill the necessity of lighter version conventional cryptography especially for 5G smart IoT devices. LWC has the provision of long range transferring of encrypted data, robustness and high level of security. It is enriched with features such as ultra high speed transmission, minimal power consumption, threat prevention, green networking and many more [16] [17] [18].

Diffie-Hellman Algorithm is an asymmetric cryptography protocol that is designed over public-key cryptographic protocol [15]. The security system is based on computational complexity of a Discrete Logarithmic Problem. Key is computed by peer users that are based on prime and generator. Then Diffie-Hellman shared secret key that is computed by peer users. But this key exchange is also vulnerable to certain attacks.

Elliptic Curve Diffie-Hellman Algorithm: Since the IoT system comprises of heterogeneous devices and network technologies such as sensors, actuators, RFID tags, smart devices, smart phones and etc. in dynamic environments [19]. But is impractical and challenging task to deploy traditional security protocols to face very powerful threats [20]. To maintain trade-off between complexity and robustness of security protocols is also highly challenging in heterogeneous environment. It is necessary to establish much secure channels while communication initiation from wireless sensor networks (WSNs) to legacy Internet system for the protection of data flow [21] [22].

It is also mandatory to provide the key management system between Internet hosts and sensor nodes for security credentials. Traditional Public Key Cryptography (PKC) is very much expensive and time consuming for resource constrained devices. Pre-shared keys used in PKC may not be convenient for dynamic IoT environment. ECC is a viable PKC system that is designed using hybrid keying mechanisms and unified in the traditional security protocols. It can also be implemented in constrained devices [23] [24].

Elliptic-Curve Diffie-Hellman key exchange algorithm is the variant of DH protocol and it makes the basis of security authentication. It is more difficult to compute the key of ECDH hence it is more secured [25]. This is power efficient and good choice for cost, bandwidth and security (authorization and authentication). ECDH protocol is used for key agreement where peer entities generate a secret key and it is used for operations which involve a private key. Public key generated by one side entity is shared with the other. ECC and ECDH algorithms have taken over the RSA in certain applications. Advantages of this algorithm are the reduced key sizes and high speed computation. Storage, Power and bandwidth are also constrained [26].

One Time Password (OTP) Algorithm: OTP algorithm is used for authentication mechanism that was opted by many researchers for designing lightweight security protocols in IoT based environment. Authors in [27] opted for asynchronous OTP. This algorithm is based on random challenge and pre-shared key. Random challenge defends the authentication against cryptanalysis attacks and replay attacks [28]. An encryption algorithm HOTP was used in [29] for computing OTP using key and the challenge.

LA1 and RA1: LA1 is chosen for authentication and verification between IoT network and device used. RA1 is opted for generating session key for encryption [6].

Radio Frequency Identifier (RFID): RFID technology was emerged by Harry Stockman in 1948, at Auto-ID centre. In 1959, RFID commercial system was originated. First transponder system was originated in 1973. First RFID chip was used in 1979 in objects. The complete implementation of RFID took place in 1999 with the origination of IoT [30]. Using this technology, devices perform functions without human assistance. One of the major tasks performed by RFID embedded devices is identification of objects [31] [32]. Other important advantage is the capability of communication with other devices and database servers that is possible using RFID tags [33]. Hence, RFID contributes a lot in development of smart environment including many smart objects [32]. RFID is used for authentication in order to provide security and privacy.

Bitwise Operations: Operations can be performed on bit level using bitwise operators. Although number of bitwise operations are available but widely used bitwise operations are (bitwise AND (&), bitwise OR (|), bitwise XOR (^) and addition mod 2m (+). These operations are simple and less costly. Others bitwise operators are costly to be used.

3. LITERATURE REVIEW

The biggest challenge for researchers in reviewed articles is security. Protocols used for communication in IoT network need to be authenticated in order to provide security artifacts. Literature review outlines various proposed secure and lightweight IoT protocols.

Pedro Peris Lopez *et al.* (2006) proposed a real lightweight mutual authentication protocol for low cost RFID tags, named as LMAP. Devices using traditional low cost RFID tags provide very low computational capabilities and out of 5K-10K logic gates, only 250-3K logic gates can be used for security purpose. Due to low cost many resources were being lacked for performing cryptographic operations. Therefore, security was a major concern. Authors studied and compared many earlier proposed solutions based on classical cryptographic approach like block cipher, hash functions, PRNG and etc. An improved low-cost RFID tag with minimal cryptography was proposed in this paper with reduced number of gates. This is an efficient lightweight protocol based on index-pseudonyms (IDSs) where each tag is associated with a key that is divided into four parts of 96 bits each.

$$(\boldsymbol{K = K1 \parallel K2 \parallel K3 \parallel K4})$$ [34]

Random number generation operations were used by reader and size of tags for security operations are less than 1K which include bitwise logical operations. Authors also outlined the working procedure of protocols. 480 bits of rewritable memory is required at the time of key and IDS updating. The proposed work has been split into four stages. First stage is mutual authentication that consists of reader authentication and tag authentication for message exchange. As soon as reader and tag mutually have been authenticated, next stage to be carried out is index-pseudonym and key updating. In third stage security evaluation is performed for confirmation of user's data and performance analysis is done using some overheads. In final stage architecture is implemented for proposed protocol. Proposed work was analyzed using five different types of word length (8, 16, 32, 64 or 96 bits) with different number of gates for bitwise operations. The main characteristic of this protocol is that for tag identification no exhaustive search is required by reader in the back end database. It is also able to avoid many security problems. Hence efficiency and security is good enough [34].

Hung-Ya Chien (2007) proposed a new ultra-lightweight RFID authentication protocol with limited resources. The proposed protocol was named as SASI as it provides protection with strong authentication and strong integrity during transmission and data updating. This protocol uses simple bit-wise operation on tags for resistance of almost all possible attacks. Author classified RFID protocols in four classes which are: Class 1 refers to Full-fledged protocols that support conventional cryptography functions such as one-way cryptographic function, symmetric cryptography and public key encryption algorithms. Class 2 called Simple class that supports one-way hash function and random number generator, Class 3 is Lightweight protocol that uses CRC checksum and simple random number generator functions and Class 4 is ultra-lightweight protocols that requires simple bitwise operators (XOR, OR AND, etc.) on the tag(s) [35].

Gildas Avoine *et al.* (2010) outlined some practical passive attacks possible on SASI and also introduced a passive full-disclosure attack to be performed against SASI in case of modular rotation. These attacks are mainly used for revealing secret ID of the user and can effect upto 2^{17} authentications. It also provides an approach to threaten ultra lightweight security protocols. Deployment of RFID raised the concern related to privacy. Authors mentioned need of the implementation of lightweight authentication protocols with low cost tags ensuring privacy. Authors in [35] [36] proposed extremely lightweight authentication protocols providing SASI and implemented using low cost tags. But these protocols were suffered from some problems like teething and weakness in design [3] [37] and were also sensitive towards some security. Authors reviewed some literatures related to SASI. They analyzed security weaknesses and highlighted possible practical passive attacks including active de-synchronization and full-disclosure attacks [38], traceability attacks due to compromised tag [39], traceability attack in order to guess least significant bit on static identifier [37], passive full-disclosure attack against SASI variants on defined rotations and full disclosure attack was proposed in discussed study that requires passive attacker to eavesdrop 2^{17} in order to disclose tag ID [3].

Thomas Kothmayr *et al.* (2013) proposed a design of secure architecture for IoT system, using DTLS protocol, to work on LoWPAN. It was mainly designed for LoWPAN. It provides a symmetric key exchange and mutual authentication for developing symmetric and secure channel. X.509 certificate [40] and RSA algorithms [41] are used for authentication. Trustworthy third parties are also needed for strong authentication. This is a robust solution but not an optimized one. High energy and time is consumed while exchange of large number of messages and DTLS handshaking. Secondly, the size of X.509 certificates is not adaptable for the

constrained devices and memorization capacity is very small [42].

Francisco Vidal Meca *et al.* (2013) proposed Host Identity Protocol (HIP), which was a security protocol for IP based IoT. The study concentrates on LoWPAN. The protocol HIP was developed using asymmetric key cryptography. Central authority was proposed to maintain and control each IoT domain. The main goal of proposed work was to add a reliable central administration for controlling and managing domains of IoT. Central authority and devices mutually authenticate each other using asymmetric cryptography when new association is established. Communication can be start only after the authentication of any two entities. Then symmetric keys of session are encrypted and shared transmission can be started. Multimedia Internet KEYing (MIKEY) protocol was proposed for key updating and management. But key generation and providing a new key on every association is a time consuming task. The proposed work was a secure architecture with flexibility that was based on HIP and MIKEY. Here HIP has been extended with capability of MIKEY [43].

Freddy K Santoso *et al.* (2015) proposed a lightweight proposition design for Wi-Fi based IoT for providing mutual authentications. According to the architecture, all communication supposed to pass through the gateway. The design is based on public keys using pre-shared keys. These keys are designed using Elliptic Curve Diffie-Hellman (ECDH) [44]. Using this, data could be securely transmitted and exchanged using a symmetric secure channel. Although this system was lightweight and energy efficient, but it was less efficient against some attacks like Denial-of-Service and cryptanalysis [45].

Mu'Away Naser *et al.* (2015) proposed SURV: Shelled Ultra-lightweight Randomized Value Authentication Protocol for Low-Cost RFID Tags. This is a protocol with high security and less computational cost. It overcomes several security pitfalls of several other protocols. It is based on the on-tag lightweight and on-reader standard cryptographic protocol. Authors in this paper include security and performance analysis and presented comparison with many other existing protocols. SURV focuses on security of the channel that connects the tag and the reader. Authors in this paper also conducted security analysis against various threats to the security of protocol. Analysis was conducted by investigation of each attack. Performance measurement of proposed protocol can be conducted by determination of storage requirements, computational cost and the security level. SURV uses simple bitwise XOR, left hamming rotation, addition mod 2% and Mix-bits function on tag. SURV is capable to provide transactions of shell values with ability of transport encapsulation encryption privacy. This protocol also guarantees the anonymity and privacy of tags while data transfer between reader and tag. Data values are not stored from previous sessions after the termination of session. Data values are also not updated in tags until all the transactions have been validated and executed completely [46].

Tewari and Gupta (2016) proposed Cryptographic-analysis of a novel ultra-lightweight protocol for mutual authentication in IoT environment for RFID tags. Main aim of this protocol was to communicate securely with less computational overhead and cost of storage. Authors also performed comparison between proposed task with other existing protocols in order to verify strength and ensuring security. An attack mechanism has also been presented with consideration of attack patterns by adversary of planning an attack on IoT. Authors in this paper discussed the history and various properties of RFID in detail. Authors used only two types of bitwise operations which are Bitwise XOR and Bitwise rotation. XOR($\oplus$) performs bitwise addition modulo 2 and Rot (A, B) makes rotation of A left by wt(B) (mod 96) where wt(B) is the hamming weight of B with the number of 1's in B. Bit length used for A is 96 bits. Server uses Random number generation along with bitwise operations.

Although the proposed protocol is efficient in terms of storage and communication cost and computation overhead is also less but the protocol is vulnerable to some attacks. Attackers can easily access the key shared between a tag and database server used on back-end. Authors considered an attack pattern for their proposed task and presented an attack mechanism including four steps: plan, deploy, monitor/detect and ex-filtrate. Proposed protocol includes three entities: tag, reader and back-end server. Authors assumed that the strength of security of the channel between back-end server and the reader is reliable but the channel is susceptible between reader and the RFID tag. Here each channel stores 96 bits tag ID, a key value and a pseudonym. It means only 96 possible rotations are possible. Here, {IDS, K} is used as a shared key by the tag and the back-end database server. The tag and the database server also store old values from previous authentication session i.e. $\{IDS_{old}, K_{old}\}$. Authors also proved security and un-traceability of their approach by performing cryptanalysis of proposed algorithm. The model is based on the Juels-Weis model [47]. Security provided by proposed protocol against some other attacks are Anonymity, Confidentiality, Integrity, Tracking, and Security against replay, man-in-middle, disclosure and de-synchronization attacks [33].

Gourinath Banda *et al.* (2016) proposed 'One Protocol', that is medium independent. Three entities of this protocol are cloud, client (may be smart-phone or any host machine) and IoT device. Using various communication media, client allows remote access to IoT devices. Cloud keeps track and mapping on number of IoT devices and it is necessary for remote hosting. Cloud network provides user accounts to keep track on devices used in IoT. Cloud also give grant and revoke permissions to authorized users to access IoT devices.

This paper also demonstrates some communication flaws related to IoT paradigm. Proposed protocol is an application layer protocol that could be accessed using different interfaces like Bluetooth/USB/NFC. It guarantees uniform communication abilities. Authors in the paper demonstrate flows of communication in IoT paradigm which are 'Invocation of operations of a thing' and 'Changes in configuration of a thing'. Prerequisite communication methods pre-used to communication flows for Discovery, Registration and Advertisement of Things. 'DISCOVERY' is a method that performs a local scan to discover available nodes using Wi-Fi, Bluetooth, Ethernet and short range protocols. But the discovery is not applicable on with IP address communication. But a User can contact with IoT devices only if it has an IP address and a key. Communication is possible after successful

registration and key authorization. 'REGISTER' is a method that is used to add new things securely on the cloud based web host and to maintain mapping between things and users. For adding new things in thing account, a user has to send the access credentials which are Thing ID and Thing key. Client can send 'REQUEST-ADDRESS' Request. User is authorized to invoke things after Registration. 'INVOKE' method is used to invoke operations of a thing. 'CONFIGURE' is a protocol method for generic and non-implementation specific configuration updates of IoT devices. Cloud services are used as static reference in absence of static IP-address of a thing.

Authors also looked into many security aspects (network, server and data) of the protocol and promised an affordable security policy that provides safety and availability. In the proposed work, an encryption should be performed for data exchange between two things and different key is used for each time for maximum protection. The protocol is universal and economic with less manufacturing and implementation cost [48].

J. Aravindh *et al.* (2017) described home automation architecture system using an open IoT protocol i.e. 6LoWPAN (used for networking) along with sensors and actuators. Authors highlighted some disadvantages of other home automation techniques such as Ethernet (wired), Zigbee and Wi-Fi (wireless), which are hindering their proper adoption. Identified Wi-Fi issues are cost, interoperability and high consumption of power. Suggested solution is implementation of 6LoWPAN (based on IPv6 and lossy network). Large number of devices can be integrated including number of IP addresses. Here the main goal is to design a robust, easy to use, low cost, flexible and full of capabilities home automation system. Main advantages of 6LoWPAN highlighted are: high scalability, long spam lifetime, and low power/fuel consumption, support to multicasting, Internet integration transparency and free licensing for IoT [49].

Mohammad Tahar Hammi *et al.* (2017) proposed a robust, energy efficient, secure, authentication, lightweight and fast protocol for protection of wireless sensor networks. The proposed work has been implemented on OCARI platform (an energy efficient and reliable WSN) that is widely used in industrial WSN. Real tests have been done for performance evaluation of proposed work. This system doesn't require new symmetric key generation every time keeping system safe against replay and cryptanalysis attacks. OTP algorithm was opted for proposed work. The system is to be kept secure against replay attacks and cryptanalysis attacks and also provide mutual authentication, integrity and confidentiality.

Authors in this paper also proposed a lightweight mutual exclusion protocol for IoT. This was a mutual authentication protocol having goodness of mechanism, for derived keys-exchange. The protocol was developed for IoT system security. Base of this protocol was pre-shared key. Though the system was a lightweight, fast and robust but there was lack of confidentiality of transmitted data. Due to the use of HMAC for packet signing, it was expensive for execution and computing time [50].

Eppy Yundra (2017) ADES was proposed to improve the performance of 802.15.4 networks in order to reduce collision and blind of back-off processes, which consume more energy for random back-off. Markov chain analysis has been included in this study for the prediction of the probability of successful communication, bandwidth utilization, network good-put and network energy utilization [51].

King-Hang Wang *et al.* (2017) proposed a work that was an improvement of ultra-lightweight mutual authentication protocol, proposed by Tewari and Gupta, for RFID tags in IoT environments [33]. Protocol was very efficient and used only two bitwise operators. Main emphasis of previous protocol was to provide secure communication with minimum computation and storage cost. But that was vulnerable to the key disclosure attacks. Key could be revealed by an adversary. There are only 96 rotation operations. The proposed protocol explored the possibility of patching for fixing the problem with few modifications. Two verification equations are R and S which are causes of vulnerability [33] and have been modified using simple improvement. Hence, new amended equations of R and S are as follows:

$$\boldsymbol{R = Rot(Rot(K, IDS \oplus n) \oplus m, K)}$$

$$\boldsymbol{S = Rot(Rot(K, IDS \oplus m) \oplus n, K \oplus R)}$$

These equations solve the problems mentioned by Tewari et. al in [33]. But cost of improved algorithm is also same as previous protocol. The amended protocol can be accessed with more number of read [52].

Won-il Bae and Jin Kwak (2017) proposed smart card based secure authentication protocol in multi-server IoT based environment. Proposed protocol can perform authentication for every connected thing (entity) by allowing users to pass through the process of authentication using a smart-card. Here data is transferred from an authenticated server for login to an IoT connected server. The security of present work is verified using a formal verification simulation with the help of a security verification tool i.e. AVISPA [2].

Venugopal and Doraipandian (2017) provided an investigation of various existing lightweight cryptographic algorithms used for security purpose. There are several security challenges in front of network connected devices users in IoT based smart environment. As already has been discussed in present paper that heavyweight security algorithms can't handle all security issues. Authors in this paper addressed variety of lightweight cryptographic algorithms. Discussed algorithms are: (1) Identity Based Encryption Scheme referred as Fuzzy IBE [53] containing capable to tolerate predefined errors, (2) Attribute-based Encryption containing non-monotonic access structure [54] that is capable to express Boolean formula but less efficiency and more complexity was a related issue, (3) An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies [55], Attribute based encryption with fast decryption algorithm used in public key cryptography where low size key is used, (4) Elliptic Curve Cryptography security [56] that was enough efficient to handle privacy and security and uses less key size, (5) lightweight authentication protocol for Internet of Things [57] that was efficient to reduce inadequacy and establishment of secure key, (6) A lightweight attribute-based encryption scheme for the Internet of Things [14] that is much efficient

and having low cost. Authors also discussed many other networks and IoT based lightweight encryption algorithms [58]-[65] and a protocol for RFID based environment. But discussed algorithms are still susceptible to various types of security related attacks [13].

Kai Fan *et al.* (2017) proposed a lightweight RFID based protocol for privacy protection of medical data in IoT. Actually security of medical data is at high risk over the years. Personal privacy of medical can be leaked by various malicious attackers. RFID technology has been used for solving the problems of medical privacy. As per earlier discussion, RFID has three parts. RFID tags are responsible for information collection. Reader can conduct data exchange process with the back-end server. The whole information interaction process is performed in cipher text form. Proposed scheme guarantees the security and privacy of collected data using secure authentication. Authors also performed performance analysis with some other schemes, As compared to many other protocols this protocol provide more efficiency of security and consumes less computational cost. BAN logic rules were used for providing for feasibility. Index data table has been adopted for improving the efficiency of information retrieval. Other operations which have been performed are random number generation by reader, cloud and tag, concatenation, XOR, PRGN and Rotation [66].

Ruhul Amin *et al.* (2018) proposed an authentication protocol based upon distributed cloud environment using smartcard. Using this protocol a registered user can securely access the private information from cloud servers. Using a cryptanalysis, it has been confirmed that protocol is secure against various security threats and it has been found superior with respect to many parameters. Authors used BAN logic for providing authentication and AVISPA tool for ensuring safety of protocol against security attacks [67].

Zhijie Ma *et al.* (2018) proposed work was to design and analysis of a distributed and demand based backscatter Medium Access Control protocol for large scale IoT networks. Devices without battery can communicate with other devices using Backscatter wireless technology. Authors considered a large scale network of IoT that consists of the legacy of backscatter and Wi-Fi communication. Proposed protocol requires collecting information of backscatter devices and enables to maintain channels with Wi-Fi devices. These devices can participate in contention in a limited period of time. Authors also expressed the throughput of backscatter and Wi-Fi devices and using simulation verified the accuracy and outperformance of proposed protocol by comparing with other protocols. Information rate is also different from ambient signals [68]. Tag can adopt two stages for detecting the backscatter (tags) transmission which are: the average envelope stage and the compute threshold stage. First stage includes Resistive/capacitive circuit and envelope detector whereas second stage includes comparator and RC circuit. FM0 coding [69] or Manchester coding [70] was adopted to overcome some carrier sense problems in physical layer [71].

Mehreen Kiran *et al.* (2018) proposed an analytical model for designing and analysis of IEEE 802.15.4 MAC based Multi-hop wireless networks for IoT based applications. Three different types of nodes have been used including leaf nodes, relay nodes and pre-gateway nodes in this model. Researchers also used the 3D Markov chains with different performance metrics [72].

Hiba A. Taresh (2018) proposed protocol was also a lightweight protocol for authentication. It was designed for security authentication of IoT and was based on LA1 and RA1 algorithms. LA1 is generally used for authentication whereas RA1 is used for secure session key generation for encryption. Each device, that is to be connected to IoT network, must be authenticated and encryption operation needs to be applied on data. A smart card, Device Identity Holder (DIH) is integrated to IoT device with Ki and GIDN numbers. Author compared IoT authentication, identification and privacy protection based on cryptography of different protocols which are useful against many types of attacks. She also compared some European Projects based on IoT security [6].

Yo-Hsuan Chuang *et al.* (2018) proposed a light-weight protocol for continuous authentication. The protocol was developed for gateway and sensing devices in IoT. Valid authentication period of time is also the concept in order to improve robustness between IoT devices. Token technique has been used for protocol construction. Dynamic IoT device features have been followed to reach goals which are reduction of power and energy consumption, time saving by reducing computational time-complexity and authentication between devices in the session. Proposed protocol claimed to be strong protocol among various competitor protocols [73].

Alireza Radan (2018) presented a protocol having two factor authentications. The proposed work is based on public-key cryptography for privacy of things and protection of IoT system against many types of attackers. Complex calculations have also been tried to diminish in order to reduce the computational complexity from O(n) to O(1), in back-end. Proposed work can protect IoT system against many attacks such as tag reading and tempering with, message replay, and man-in-middle attack. Cryptography algorithms used here are: ECC public keys (keys with different sizes) and Robin. Security against tag tracking attack is also an important advantage of proposed protocol. Test application area to examine results is toll paying in traffic management [74]. MATLAB has been used as simulation environment for implementation. The main aim of this research is to design a RFID based mutual authentication protocol for the system based on public-key cryptography algorithms (RSA, ECC and ElGamal). Authors in [75] also discussed about security of smart environment for RFID [76].

Stefan Marksteiner *et al.* (2018) presented a study of various wireless IoT protocols security in smart home environment. Protocol's security is also an issue in smart environment. In this study, authors discussed and compared many wireless protocols including Z-Wave, Zigbee, EnOcean, Thread, and KNX-RF. These all have encryption, authentication checking services using AES. Authors presented security protocol with a better understanding of all 7 layers in OSI model corresponding to 4 layers in TCP/IP model. Researchers mainly focused on security implications of protocols existing on transport and network layer. AES algorithms have been used for encryption

with 128 bits key length. Many other encryption algorithms, authentication algorithms and key exchange algorithms have also been explored for security purposes [77].

Li Celia and Yang Cungang (2018) recently proposed a protocol with secure and effective key management feature. The presented protocol also follows interactive key management as well as non-interactive key management to minimization of communication cost in Io-T based environments. This work is also containing many security features to protect against many types of attacks [78].

En-Cheng Liou *et al.* (2018) called reader's attention towards Internet of Under-water things (IoUT) protocols and many challenges. Actually wireless sensor network is the base of application area. Researchers in this paper provided an investigation of cutting edge routing protocols and also highlighted some communication challenges [79].

4. COMPARATIVE ANALYSIS OF DIFFERENT REVIEWED PROTOCOLS

Table 1 shows comparative analysis of some of recently proposed protocols. These protocols have been briefly reviewed in the present paper. Table 1 also includes algorithm(s), technique(s), key size or rotations used by a protocol. Hence, comparative analysis has been performed in terms of Algorithms, tools, techniques and key size used for different protocols as well as their feature and research gaps also have been shown.

Table 1: Comparative Analysis of Different Reviewed Protocol

Proposed Work	Algorithm(s) Used	Tools, Techniques and Other Requirements	Key Size/ Rotations	Features	Research Gaps
LMAP (2006) [34]	• Index Pseudonyms • PRNGs	Bitwise Logical (AND, OR, XOR and mod2^m)	4 keys of 96 bits each	• Very low cost • efficiently handle security problems • attack tracking-man-in-middle forwarding replay • security promising	• Not resistant to disclosure and de-synchronization attacks • Lack of anonymity, • Lack of mutual authentication and forward secrecy in different cases
SASI (2007)[35] **SASI) is not that Strong (2010) [3]**	•RNG •IDS	•Very low cost RFID • Basic bit-wise operations (AND, OR, XOR, Rot) •Modular Addition •300 gates	$ID = IDS = K1 = K2$ of 96 bits	• very low cost • strong authentication • strong integrity • resist many attacks • access control, • robustness • secures constrained devices	• RFID may be unprotected against DoS like attacks • Unprotected RFID information can be gathered illegally • Threats and passive attacks possible on privacy • Easy to reveal secret ID by eavesdrop
HIP (2013) [43]	•RSA: Asymmetric Key Cryptography •Cryptographic key hash •Public key exchange authentication •Kerberos: Symmetric Key Cryptography	•LoWPAN •IPv4 and IPv6 •Dynamic addresses •Sharing of session symmetric keys •MIKEY	128 bits hash to identify host	• Carries data with good authentication and encryption • Mobility and location privacy • Central authority • Mutually authenticated	•Requires very complex environment •Multiple interface host is very challenging •Energy and time consuming in some applications
DTLS based security Protocol (2013) [42]	•RSA •x.509 certificates	•LoWPAN •Trustful third party is required for authentication •Symmetric key exchange	1024 bit, 2048 bits and can also vary	• Mutual authentication • Robustness • Ensures strong authentication • Confidentiality • Integrity	•Size of x.509 is not adaptable •Energy consuming • Time consuming execution • Small capacity of memorization
Lightweight Proposition for	ECDH	Wi-Fi based	Public keys combined with	• Mutual authentication • Lightweight	• Less secure against Denial of Service attack

Wi-Fi based IoT Security Protocol (2015) [45]			Pre-shared keys	• Energy efficient • Reasonable computing capacity • Integrity	• Cryptanalysis attack
SURV (2015) [46]	Binary Search	• Simple Bitwise operations (XOR, addition, • Hamming rotation • Mix-bits function	Common secret keys of variable size	• Resistant to de-synchronization and disclosure attacks • Provides privacy and security • Authentication • Channel security	• Vulnerable to some attacks
Novel Ultra-Lightweight Mutual authentication protocol (2017) [33]	• RFID Tags • Random number generation	• Bitwise XOR • Bitwise rotation	96 rotations	• Secure communication and data transmission • low cost (storage and computation) • Integrity • Anonymity • Tracking • Confidentiality • Forward secrecy • Security against replay, man-in-middle, disclosure and de-synchronization attacks	• Vulnerability • Attacker can obtain the key b/w back-end database server and tag
One IoT (2017) [48]	Salted Data encryption	• Key authorization • Data encryption, Device discovery • Registration, advertisement • Invocation • Configuration	128 bits	• Affordable security, • Robustness • Increased entropy of cipher-text with salt • DDos identification and prevention • Flexibility • Unconditional compatibility	• Very personalized • Very specific to applications • Can't perform registration if current IP address is not known • Strong but complicated process • Switched to different frameworks
Smart Card based Secure Authentication Protocol (2017) [2]	• One-way • XOR functions	• AVISPA Tool for verification	Key Size can vary	• Security against impersonation attacks and session key disclosure attacks • Dos attack • Server spoofing • Privacy invasion • Applicable in key exchange	• Very specific to applications • Vulnerable to some attacks
Lightweight Cryptographic Solution for IoT (2017) [13]	• ECC • ECDH algorithms	• RFID Tags • Combined asymmetric and symmetric cryptography	ECC (224 bits – 2048 bits) ECDH (2048 bits)	• High efficiency • Adequate security level in data transmission • Reduced computational and communicational cost	• Vulnerable to some attacks
Lightweight Mutual Authentication Protocol (2017) [28]	HMAC	• OCARI (WSN) platform for protocol implementation • Mutual data authentication and encryption	Pre-shared keys	• Low cost • Data authentication • Robustness • Energy efficient • High speed	• Lack of confidentiality in data transmission

A Lightweight IoT Security Protocol (2017) [9]	• HMAC • OTP	• Asynchronous OTP • Random challenge • OCARI • Scyther tool	Pre-shared key, AES,	• Energy efficient • Lightweight and robust, authentication • Encrypted data exchange, authentication against replay, confidentiality, integrity	• Vulnerable to some attacks
New Ultra Lightweight Authentication Protocol (2017) [52]	RFID Tags	• Bitwise operation XOR • Random Shift	96 rotations	• Improved security algorithm • More secure communication • Secure against key disclosure	• Increased no. Of read than previous • More no. Of rounds of interaction with tag
Wireless IoT Protocol Security in the Smart Home Domain (2017) [77]	• AES • HMAC • CMAC_AES • AES_CCM	• Zigbee • Z-Wave • EnOcean • KNX • Thread	128 bits	• Provides security (Integrity, Authentication) in Smart home domain • Replay Protection	• Sometimes less practical, • KNX lacks some security services, • Z-Wave is less explored • Zigbee is vulnerable
Lightweight RFID Protocol for Medical Privacy Protection in IoT (2018) [66]	• RNG(reader, tag and cloud) • PRNG • Bitwise XOR • Concatenation Cross • Rotation	RFID	Key Size can vary	• Security against dos, • Tag anonymity • Synchronization • Mutual authentication • Forward Secrecy • Resistant Replay Attack	• Application specific • Can't be implemented in other areas
A new lightweight authentication protocol in IoT environment for RFID tags (2018) [52]	• Public- key cryptography • RSA • ECC, • Round Robin • Anti collision algorithm of Q-Protocol	• MATLAB • RFID based system • DFSA • ALOHA	Rabin- 512 and 1024 bit, ECC- 233 bit	• Provide protection against tag reading and tag tracking, message replay man-in-middle attacks • Traffic management, • Provides mutual cryptographic authentication • Reduces complexity • Secure communication channel	• Not much suitable for Stochastic challenges • O(1) time is taken only for tag authentication while tag tracking, • Computational complexity in back-end server
Lightweight authentication protocol for IoT enabled devices in distributed cloud computing environment (2018) [67]	• Hash functions • Session key computation	• Distributed Cloud computing environment • AVISPA tool • BAN logic model	Key Size can vary	• Cloud security • Mutual Authentication • Protection against threats • Cryptanalysis	• Vulnerable to some attacks • Cloud specific
Distributed Demand Based MAC Protocol for IoT Networks (2019) [71]	• FM0 coding • Manchester coding for carrier sense	• Backscatter (tag) • Wi-Fi • Self-interference cancellation (SIC) • ADC and DCA converter • LoRa network • NB-IoT	Size varies according to application	• More accurate • More throughput • access point can decode the received signals using sic technique • Distributed mac protocol maintain large information • Helpful calculate per node throughput of backscatter and wi-fi devices	• Efficiency of backscatter communication is less than wi-fi • Half-duplex access point can't be achieved or half-duplex ap is nor suitable

5. CONCLUSION

The present review primarily focuses on the security requirements of IoT. The literature review summarizes the primitives of lightweight security protocols for IoT enabled smart environment. Various existing lightweight protocols proposed by researchers have also been discussed. The present paper also highlights the features and limitations of discussed protocols. This paper can be useful as a reference for designing and implementing lightweight security algorithms. The features discussed and the research gaps identified are expected to be very helpful for designing a new improved protocol.

REFERENCES

[1] C. Kolias, W. Meng, G. Kambourakis and J. Chen. **Security, Privacy, and Trust on Internet of Things**, Wireless Communications and Mobile Computing Vol. 2019, Article ID 6452157, 3 February 2019. W. Bae and J. Kwak. **Smart card-based secure authentication protocol in multi-server IoT environment**, In Multimedia tools and applications, pp.1-19, 26 December 2017. https://doi.org/10.1155/2019/6452157

[2] G. Avoine, X. Carpent and B. Martin. **Strong Authentication and Strong Integrity (SASI) is not that Strong**, RFIDSec'10 Proceedings of the 6th international conference on Radio frequency identification: security and privacy issues, pp. 50-64, June 08 - 09, 2010. https://doi.org/10.1007/978-3-642-16822-2_5

[3] Kevin Ashton. **That "Internet of Things" thing**. RFID J., Last accessed: August 2016, Available at: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf.

[4] D. Sehrawat and N. S. Gill. **Security Requirements of IoT Applications in Smart Environment**, Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018) IEEE Conference Record: # 42666; IEEE Xplore ISBN:978-1-5386-3570-4, pp. 324-329, 2018. https://doi.org/10.1109/ICOEI.2018.8553681

[5] H. A. Tarish. **Proposed Lightweight Protocol for IoT Authentication** Iraqi Journal for Computers and Informatics (IJCI) Published by University of Information Technology and Communications (UOITC), pp. 1-8, September 2018.

[6] H. Suo, J. Wan, C. Zou and J. Liu. **Security in the internet of things: A review**, International Conference on Computer Science and Electronics Engineering (ICCSEE), Vol. 3. IEEE, pp. 648–651, 2012. https://doi.org/10.1109/ICCSEE.2012.373

[7] D. Airehrour, J. Gutierrez, and S. K. Ray. **Secure routing for Internet of things: A survey**, Journal of Network and Computer Applications, Vol. 66, pp. 198–213, May 2016. https://doi.org/10.1016/j.jnca.2016.03.006

[8] Mohd. T. Hammi, E. LiVol.ant, P. Bellot, A. Serhrouchni, and P. Minet, **MAC sub-layer node authentication in OCARI**, In 2016 IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), pp. 1-6, Nov 2016. https://doi.org/10.1109/PEMWN.2016.7842906

[9] W. Qiuping, Z. Shunbing, and D. Chunquan. **Study on key technologies of Internet of Things perceiving mine**, First International Symposium on Mine Safety Science and Engineering Procedia Engineering, Vol. 26, pp. 2326–2333, Dec 2011. https://doi.org/10.1016/j.proeng.2011.11.2442

[10] W. Zhou, Y. Zhang, and P. Liu. **The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved**, IEEE Internet of Things Journal, pp. 1-11, 15 June 2018.

[11] S. Hameed, F. I. Khan and B. Hameed. **Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review**, Journal of Computer Networks and Communications Vol. 2019, No. 11, Article ID 9629381, pp. 1-14, 2019. https://doi.org/10.1155/2019/9629381

[12] M. Venugopal and M. Doraipandian. **Lightweight Cryptographic Solution for IoT- An Assessment**, International Journal of Pure and Applied Mathematics, Vol. 117, No. 16, pp. 511-516. ISSN: 1311-8080, 2017.

[13] X. Yao, Z. Chen, and Y. Tian. **A lightweight attribute-based encryption scheme for the Internet of Things** Future Generation Computer Syst., Vol. 49, pp. 104– 112, 2015. https://doi.org/10.1016/j.future.2014.10.010

[14] W. Diffie and M. Hellman. **New Directions in Cryptography**, IEEE transactions on Information Theory, Vol. 22, No. 6, pp. 644-654, 1976. https://doi.org/10.1109/TIT.1976.1055638

[15] E. R. Naru , H. Saini and M. Sharma. **A recent review on lightweight cryptography in IoT**, 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp.887-890, 10-11 Feb. 2017. https://doi.org/10.1109/I-SMAC.2017.8058307

[16] M. Alizadeh, J. Shayan, M. Zamani, and T. Khodadadi. **Code analysis of lightweight encryption algorithms using in RFID systems to improve cipher performance**, 2012 IEEE Conference on Open Systems, pp. 1-6, 21-24 Oct. 2012. https://doi.org/10.1109/ICOS.2012.6417641

[17] N. A. Gunathilake, W. J. Buchanan and R. Asif. **Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications**, IEEE 5th World Forum on Internet of Things, At Limerick, Ireland, pp. 1-5, April 2019.

[18] D. Hankerson, A. J. Menezes and S. Vanstone. **Guide to Elliptic Curve Cryptography**, Springer Science & Business Media, 2004 Springer-Verlag New York, Inc., pp. 1-332, 2004.

[19] D. Jao. **Elliptic Curve Cryptography,** Handbook of Information and communication security, pp. 35-57, 2010. https://doi.org/10.1007/978-3-642-04117-4_3

[20] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos. **Key Management Systems for Sensor Networks in the Context of the Internet of Things**, Journal Computers & Electrical Engineering, Vol. 37 Issue 2, pp. 147–159, March 2011. https://doi.org/10.1016/j.compeleceng.2011.01.009

[21] L. Zhou and H.C. Chao. **Multimedia Traffic Security Architecture for the Internet of Things**, IEEE Network, Vol. 25, No. 3, 2011, pp. 35-40, 2011. https://doi.org/10.1109/MNET.2011.5772059

[22] A. Liu and P. Ning. **TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks**, In: 7th international conference on Information processing in sensor networks, IEEE Computer Society, ISBN: 978-0-7695-3157-1, , pp. 245-256, 22-24 April 2008.

[23] Z. Liu and H. Seo. **IoT Nums-Evaluating NUMS elliptic curve cryptography for IoT platforms**, IEEE Transactions on Information Forensics and Security, Vol. 14 , Issue 3, pp. 720-729, March 2019. https://doi.org/10.1109/TIFS.2018.2856123

[24] P. Porambage. **Lightweight Authentication And Key Management Of Wireless Sensor Networks For Internet Of Things**, Academic dissertation to be presented with the assent of the Doctoral Training Committee of Information Technology and Electrical Engineering of the University of Oulu for public defence in Kaljusensali (KTK112), Linnanmaa, pp. 1-74, 26 September 2018.

[25] R. K. Kodali and A. Naikoti. **ECDH based Security Model for IoT using ESP8266**, 2016 International conference on control, instrumentation, communication and computational technologies (ICCICCT), pp. 629-633, December 2016. https://doi.org/10.1109/ICCICCT.2016.7988026

[26] E. Sediyono, K. I. Santoso and Suhartono. **Secure login by using One-time Password authentication based on MD5 Hash encrypted SMS**, 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp.1604-1608, 22-25 Aug. 2013. https://doi.org/10.1109/ICACCI.2013.6637420

[27] M. T. Hammi, E. Livolant, P. Bellot, A. Serhrouchni and P. Minet. **A lightweight mutual authentication protocol for the IoT**, ICMWT: International Conference on Mobile and Wireless Technology, pp. 3-12, Technical report, 17 June, 2017, HAL Id: hal-01640510, Version 1, available on https://hal.archives-ouvertes.fr/hal-01640511. https://doi.org/10.1007/978-981-10-5281-1_1

[28] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen. **HOTP: An HMAC-based one-time password algorithm**, Network Working Group IETF, RFC Informational 4226, December 2005, pp.1-37, Last updated 20th December 2018. https://doi.org/10.17487/rfc4226

[29] Near Field Comminications History, **Timeline of RFID technology**. Available on http://www.nfcnearfieldcommunication.org/timeline.html, July 2016.

[30] Postscapes, **History of Internet of things**. Available on http://postscapes.com/internet-of-things-history. Last accessed July 2016.

[31] Buckley J (ed). **The Internet of things: from RFID to the next-generation pervasive networked systems**, Auerbach Publications, New York, 2006.

[32] A. Tewari, B.B.Gupta. **Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags**, Journal of Supercomputing, Vol. 73, No. 3, August 2016. https://doi.org/10.1007/s11227-016-1849-x

[33] P. P. Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda. **LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags**, Proc. of Second Workshop on RFID Security, Vol. 6, July 2006.

[34] H. Y. Chien. **SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity**, IEEE transactions on dependable and secure computing, Vol. 4, Oct-Dec 2007, pp. 337-340. https://doi.org/10.1109/TDSC.2007.70226

[35] P. P. Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda. **EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags**, Proc. OTM Federated International Conferences, On the Move to Meaningful Internet Systems, pp. 352-361, October 2006. https://doi.org/10.1007/11915034_59

[36] T. Cao, E. Bertino, and H. Lei. **Security Analysis of the SASI Protocol**, IEEE Transactions on Dependable and Secure Computing, TDSC-2008-01-0021, Vol. 6, Issue 1, pp. 73-77, January 2009. https://doi.org/10.1109/TDSC.2008.32

[37] P. D'Arco and A. D. Santis. **Weaknesses in a Recent Ultra-Lightweight RFID Authentication Protocol**, Proceeding AFRICACRYPT'08 Proceedings of the Cryptology in Africa 1st International conference on Progress in Cryptology, pp. 27-39, 11-14 June, 2008. https://doi.org/10.1007/978-3-540-68164-9_3

[38] H. M. Sun, W. C Ting, and K. H. Wang. **On the Security of Chien's Ultra-Lightweight RFID Authentication Protocol**, IEEE Transactions on Depend-able and Secure Computing, Vol. 8, No.2, March 2011, pp. 315-317. https://doi.org/10.1109/TDSC.2009.26

[39] F. Forsby, M. Furuhed, P. Papadimitratos. **Lightweight X.509 Digital Certificates for the Internet of Things**, Third International Conference, InterIoT 2017, and Fourth International Conference, SaSeIot 2017, Valencia, Spain, pp. 123-133, November, 2017. https://doi.org/10.1007/978-3-319-93797-7_14

[40] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, **Security and privacy aspects of low-cost radio frequency identification systems**, Security in Pervasive Computing LNCS 2802, pp 201–212, 2004. https://doi.org/10.1007/978-3-540-39881-3_18

[41] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, **DTLS based security and two-way authentication for the Internet of Things**, Journal of Ad Hoc Networks, Vol. 11, Issue 8, pp. 2710–2723, Nov. 2013. https://doi.org/10.1016/j.adhoc.2013.05.003

[42] F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, O. G. Morchon, S. S. Kumar, and S. L. Keoh. **HIP security architecture for the IP-based Internet of Things**, In 27th International Conference on Advanced Information Networking and Applications (WAINA), pp. 1331–1336. IEEE, July 2013.

[43] P. Singh and N. S. Gill. **A Secure and Power-Aware Protocol for Wireless Ad Hoc Networks**, Vol. 8, N0. 1, pp. 34-41, Jan-Feb 2019. https://doi.org/10.30534/ijatcse/2019/07812019

[44] F. K. Santoso and N. C. Vun. **Securing IoT for smart home system**, In 2015 IEEE International Symposium on Consumer Electronics (ISCE), pp. 1–2, June 2015. https://doi.org/10.1109/ISCE.2015.7177843

[45] M. Naser, Y. Alshamaila, R. Budiarto, and P. P. Lopez. **SURV: Shelled Ultralightweight Randomized Value Authentication Protocol for Low-Cost RFID Tags**, International Journal of Computer and Electrical Engineering, Vol.7, No.3, pp. 206-214, June 2015. https://doi.org/10.17706/IJCEE.2015.7.3.206-214

[46] A. Juels and S. A. Weis. **Defining strong privacy for RFID**, Journal of ACM Transactions on Information and system security (TISSEC), Vol. 13 Issue 1, pp 342–347, October 2009. https://doi.org/10.1145/1609956.1609963

[47] G. Banda, C. K. Bommakanti and H. Mohan. **One IoT: An IoT Protocol and Framework for OEMs to make IoT devices forward compatible**, Journal of Reliable Intelligent Environments, Vol. 2 Issue 3, pp.131–144, Springer International Publishing Switzerland Nov. 2016. https://doi.org/10.1007/s40860-016-0027-5

[48] J. Aravindh, V. B. Srevarshan, R. Kishore and R. Amirthavalli. **Home Automation in IoT using 6LOWPAN**, International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Vol. 5, Issue 5, pp. 26-28, May 2017.

[49] M. T. Hammi, E. Livolant, P. Bellot, A. Serhrouchni, and P. Minet. **A Lightweight IoT security protocol**, HAL-01640510, version 1, 1st Cyber Security in Networking Conference (CSNet2017), Rio de Janeiro, Brazil, Oct 2017. https://doi.org/10.1109/CSNET.2017.8242001

[50] E. Yundra. **Study of Adjustment Delay Scheme on IEEE 802.15.4 Networks at Beacon Enabled Mode**, The 2nd Annual Applied Science and Engineering Conference (AASEC 2017), IOP Conference Series: Materials Science and Engineering, Vol. 288, Conference 1, pp.1-8, 2017. https://doi.org/10.1088/1757-899X/288/1/012065

[51] K. H. Wang, C. M. Chen, W. F. and T. Y. Wu. **On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags**, Journal of Supercomputing, 2017. Vol. 74, pp. 65-70, 2017. https://doi.org/10.1007/s11227-017-2105-8

[52] A. Sahai and B. Waters. **Fuzzy identity-based encryption**, EUROCRYPT'05 Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques, pp. 457–473, 22- 26 May 2005. https://doi.org/10.1007/11426639_27

[53] R. Ostrovsky, A. Sahai and B. Waters. **Attribute-Based Encryption with Non-Monotonic Access Structures** CCS'07, Proceedings of 14th ACM Conference on Computer Communication Security, pp. 195-203, October 2007. https://doi.org/10.1145/1315245.1315270

[54] P. Junod and A. Karlov. **An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies**, Proceedings of tenth Annual ACM Workshop on Digital rights Management - DRM '10, pp. 13-24, 04 October 2010. https://doi.org/10.1145/1866870.1866875

[55] P. Shruti and R. Chandraleka. **Elliptic Curve Cryptography Security in the Context of Internet of Things**, Vol. 8, no. 5, pp. 90–93, 2017.

[56] J. Y. Lee, W. C. Lin, and Y. H. Huang. **A lightweight authentication protocol for Internet of Things**, 2014 International Symp. Next-Generation Electron. ISNE 2014, pp. 1–2, 2014. https://doi.org/10.1109/ISNE.2014.6839375

[57] J. P. Vilela, L. Lima, and J. Barros, **Lightweight Security for Network Coding.pdf**, pp. 1750–1754, 2008. https://doi.org/10.1109/ICC.2008.336

[58] C. Chen, Z. Zhang, and D. Feng. **Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost**, International Conference on Provable Security, Vol. 6980 LNCS, pp. 84–101, 2011. https://doi.org/10.1007/978-3-642-24316-5_8

[59] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and Konstantios Rantos. **Lightweight Cryptography for Embedded Systems- A Comparative Analysis**, Proceeding Revised Selected Papers of the 8th International Workshop on Data Privacy Management and Autonomous Spontaneous Security, Vol. 8247, pp. 333-349, 12-13 September 2013. https://doi.org/10.1007/978-3-642-54568-9_21

[60] M. Katagi and S. Moriai. **Lightweight cryptography for the Internet of Things**, Sony Corp., pp. 7–10, May 2012.

[61] S. Ju. **A lightweight key establishment in wireless sensor network based on elliptic curve cryptography** 2012 IEEE International Conference on Intelligent Control Automatic Detection High-End Equip., pp. 138–141, 27-29 July 2012. https://doi.org/10.1109/ICADE.2012.6330115

[62] H. Kumar and A. Singh. **Internet of Things : A Comprehensive Analysis Implementation through Elliptic Curve Cryptography Security**, Vol. 6, No. 2, pp. 498– 502, 2016.

[63] S. Hohenberger and B. Waters. **Attribute-based encryption with fast decryption** Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), Vol. 7778 LNCS, pp. 162–179, 2013. https://doi.org/10.1007/978-3-642-36362-7_11

[64] K. Rhee, J. Kwak, S. Kim and D. Won. **Challenge-response based RFID authentication protocol for distributed database environment**, International Conference on Security in Pervasive Computing SPC 2005, pp. 70–84, 2005. https://doi.org/10.1007/978-3-540-32004-3_9

[65] K. Fan, W. Jiang and Y. Yang. **Lightweight RFID Protocol for Medical Privacy Protection in IoT**, IEEE Transactions on Industrial Informatics (TII-17-2052), 1551-3203, pp. 1-11, 2018.

[66] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal and V. Chang. **A lightweight authentication protocol for IoT enabled devices in distributed cloud computing environment**, Future generation computer systems, Vol. 78, Part 3, pp. 1005-1019, Jan 2018. https://doi.org/10.1016/j.future.2016.12.028

[67] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith. **Ambient backscatter: wireless communication out of thin air**, In ACM SIGCOMM Computer Communication Review, Vol. 43 Issue 4, pp. 39–50, October 2013. https://doi.org/10.1145/2534169.2486015

[68] Y. Liu, C. Huang, H. Min, G. Li, and Y. Han. **Digital correlation demodulator design for RFID reader receiver**, Proceedings of the 2007 IEEE Wireless Communications and Networking Conference, 01-15 March 2007, pp. 1664–1668. https://doi.org/10.1109/WCNC.2007.313

[69] https://en.wikipedia.org/wiki/Manchester_code.

[70] Z. Ma, L. Feng, and F. Xu. **Design and Analysis of a Distributed and Demand-based Backscatter MAC Protocol for Internet of Things Networks**, IEEE Internet of Things Journal, pp. 2327-4662, Sept. 2018. https://doi.org/10.1109/SmartIoT.2018.00012

[71] M. Kiran, R. V. P. Yerra, P. Rajalakshmi. **Modeling and Analysis of IEEE 802.15.4 Multi-hop Networks or IoT Applications**, Wireless Personal Communications: An International Journal, Springer Link, Vol. 100, Issue 2, pp. 429-448, May 2018. https://doi.org/10.1007/s11277-017-5082-6

[72] Y. H. Chuang, N. W. Lo, C. Y. Yang and S. W. Tang. **A Lightweight Continuous Authentication Protocol for the Internet of Things**, Vol. 18, No. 4. pp.1-26, Apr. 2018. https://doi.org/10.3390/s18041104

[73] E. Jome. **Evaluation of effect of security methods on efficiency parameters of RFID system for application of violations record and urban traffic management**, MSc thesis in Information Technology Engineering (Computer Network Orientation), Science and Industry University of Iran, Computer Engineering School , 2013.

[74] M. Devi and N. S. Gill. **Performance Evaluation of Dynamic Source Routing Protocol in Smart Environment**, International Journal of Advanced Trends in Computer Science and Engineering, Vol. 8, No. 2, pp. 333-338, March-April 2019.

[75] A. Radan, H. Samimi and A. Moeni. **A new lightweight authentication protocol in IoT environment for RFID tags**, Inernational Journal of Engineering and Technology, Vol. 7, No. 4.7, pp. 344-351, 2018. https://doi.org/10.14419/ijet.v7i4.7.23028

[76] S. Marksteiner, V. J. Exposito, H. Vallant and H. Zeiner, **An Overview of Wireless IoT Protocol Security in the Smart Home Domain**, 13th CTTE and Jan 10th CMI Conference on Internet of Things Business Models, Users, and Networks, Copenhagen, 2017, pp. 1-8, Available on http://ieeexplore.ieee.org/document/8260940/

[77] L. Celia, Y. Cungang. **(WIP) Authenticated Key Management Protocols for Internet of Things**, 2018 IEEE International Congress on Internet of Things (ICIOT), September 2018. https://doi.org/10.1109/ICIOT.2018.00024

[78] E. C. Liou, C. C. Kao, C. H. Chang, Y. S. Lin and C. J. Huang. **Internet of underwater things: Challenges and routing protocol**s, 2018 IEEE International Conference on Applied System Invention (ICASI), 13-17 April 2018. https://doi.org/10.1109/ICASI.2018.8394494