International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 7, No.2 (Mar-2018)
http://dx.doi.org/10.12785/ijcds/070206

Internet of Things Security Issues, Threats, Attacks and Counter Measures

Adil Bashir[1] and Ajaz Hussain Mir[1]

[1]*Department of Electronics and Communication Engineering, National Institute of Technology Srinagar, Jammu & Kashmir, India*

Received 11 Oct. 2017, Revised 30 Nov. 2017, Accepted 26 Jan. 2018, Published 1 Mar. 2018

Abstract: Internet of things (IoT) is gaining popularity now-a-days as it is revolutionizing the world of internet and physical systems in a more advanced and technical way. IoT consists of physical things in which sensing, processing and communication capabilities are added. These devices have restricted resources and processing competences. The networks formed from these miniature devices have a lot of scope and applications that include healthcare, industrial automation, military surveillance, forest fire detection, flood alarming system, smart homes, smart cities etc. Most of these applications demand secure transmission of sensed information from source IoT node to gateway node or broker. Thus, it is imperative to pay attention to the security of these networks as they are highly susceptible to risks because of wireless medium used for communication and the constrained nature of these devices. In this paper, we have presented a variety of attacks that can harm the fidelity of transmitted information in IoT, thereby generating unauthorized effects. Furthermore, various counter measures against these possible attacks that have been proposed in the literature with their merits and demerits are presented, together with possible research opportunities for future work.

Keywords: Internet of Things Security, MQTT, CoAP, RPL, Wireless Sensor Networks.

1. INTRODUCTION

T Internet of Things (IoT) encompasses a large set of devices compromising of sensing, computation and communication components having resource restrictions [1]. These devices are capable of sensing, monitoring, self-organizing and find their usage to sense the ambient condition of its environment, assemble data, and process it to extract some significant information that can be used to identify the event in the region of its surroundings. A node is the prime component of IoT network which is built of sensing, computation and wireless communication components with an on-board battery. Internet of Things lets devices to act automatically to events and changes in their surroundings without any human interaction [2]. Due to small size, quick and easy deployment and low cost of IoT nodes, it becomes possible to deploy them in a hefty area to be examined [3]. IoT nodes are typically spread over the area to be observed to collect data, process it, and forward it to the gateway directly or through multi-hop communication for further processing. Cisco estimates that the Internet of Things will grow to almost 50 billion installed units by 2020 [4]. Advances in communication technology and Micro-Electro-Mechanical Systems (MEMS) result in lowering deployment and maintenance costs of IoT and reduces susceptibility rate of node to failures with an improved battery power. Therefore, these networks find their applications in monitoring smart homes [5] or healthcare [6], assisted living, enhanced learning [7], supply chain management etc. For example, a smart door lock installed at home/apartment communicates its status to the user's smart-phone. The user can access the status of smart door lock sensor from anywhere in the world which enables him to verify, for example, if he forgot to lock the door of house before leaving, or if a robbery was attempted.

Internet of Things has a three layered architecture [8]. The three layers include Physical/ perception layer, network layer and application layer.A typical IoT architecture looks as illustrated in Figure 1.

The Physical layer or perception layer has sensors for accumulating data from environment. It senses physical parameters and shares this collected data to other smart objects. Low energy communication protocols and technologies such as IEEE 802.15.4 [9] [10], ZigBee [11], ISA 100.1a [12], WirelessHART [13] are utilized to transmit sensed data to other IoT objects.

Network layer consists of low-power routing protocols such as RPL (Routing Protocol for Low power and Lossy Networks) [14] for communication with other IoT nodes. Usually gateways are used between local

E-mail:adilbashir.445@gmail.com, ahmir@nitsri.net

sensors and Internet to connect every IoT device with each other and to the internet in general.

Application layer consists of IoT middleware and defines many applications in which IoT can be deployed like smart cities, industries, transportation, smart buildings, etc. Protocols used at the application layer include Constrained Application Protocol (CoAP) [15], Message Queue Telemetry Transport (MQTT) [16], Advanced Message Queuing Protocol (AMQP) [17], Data Distribution Service (DDS) [18]. These protocols are meant to be used for resource constrained networks like IoT.

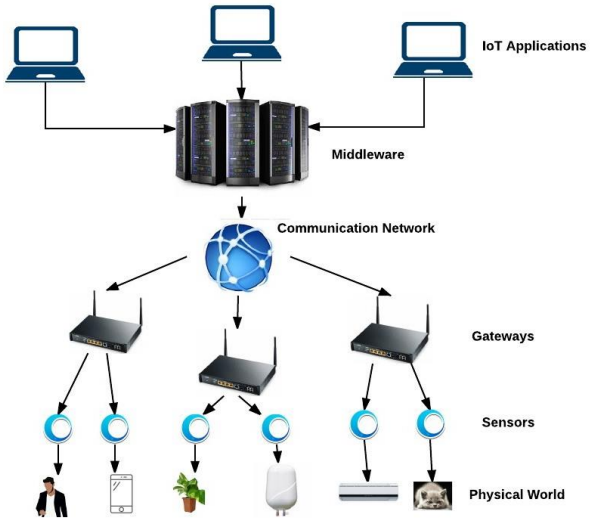

Figure 1. Internet of Things Architecture

The resource constrained nature of IoT devices induces several challenges in its design and functioning, thereby diminishing their performance. These challenges comprise of fault-tolerance, communication management, network lifetime and unwatched operational state [19], Interoperability [20], Service orchestration [21], Security & Privacy [22] [23], Standardization [24]. Hence, on one side, to ameliorate the performance of IoT, these challenges are to be investigated. While on other side, the performance of IoT can be realized appreciably by efficient resource consumption. This can be improved by concentrating on factors involved in its operations. Communication in IoT has strong influence on its resource utilization and consumes about 80% of the total available energy. Communication pattern in IoT include transmission from hop to hop or source node to target node. These communications involve optimum route determination, route maintenance, secure communication and different other operations to contend with user expectation and reasonable network performance [25]. IoT is prone to distinctive sorts of assaults as a result of wireless connectivity, lack of physical defense, the unattended nature, constrained nature and so forth. Therefore, paying attention to security aspects in IoT is extremely important.

The rest of the paper is organized as follows. In Section II, we present the security issues in IoT. Security attacks and their classification are discussed in section III. Section IV discusses about the various security protocols that have been proposed to deal with likely attacks. Finally, the conclusion of the paper is provided in Section V.

2. SECURITY IN IOT

Since IoT contrasts from different wireless or wired networks in a number of ways and the configuration and operation of these networks pose distinctive security challenges. The different security concerns in IoT are presented in this section.

Because of intrinsic restrictions on processing capabilities and available resources, security in IoT pose diverse challenges than in traditional networks. First and foremost, contrasting traditional networks, IoT devices are usually deployed at places that are accessible to anyone, therefore, making them prone physical attacks. Second, IoT devices interact with their physical surroundings and with individuals, thus, posing new security challenges. And third, a large number of the early proposed network procedures expected that all networks are cooperative and reliable. However, this is not the situation for IoT applications which oblige a certain measure of trust in the application in order to maintain proper network functionality. Implementing security is a difficult task in IoT due to their limited computational capabilities, critical security requirements and distinctive qualities as compared to other wireless networks like cellular or mobile ad hoc network (MANETs). Further the heterogeneity of devices that are connected to IoT network makes it hard to deal with security and privacy issues broughtup by new connecting devices [26].

There are three primary issues that make IoT hard to secure against attacks. First and foremost issue is the mode of communication used in these networks, which makes it difficult to protect the transmitted information. Contrasting wired systems, where a device must be physically associated with the communication channel, the wireless medium is open and available to anybody.

The second issue is nonexistence of any permanent infrastructure and specifically, there is no central controller to examine the operation of network and observe the information being exchanged. While most of these networks have a gateway node, but the job of it is just to accumulate information and transmit it to server without serving as a definite control node. Thus, any security mechanism must be executed as an agreeable, distributed exertion of all or many nodes together in the network. The difficulty in implementing security procedure in IoT increases further due to unstable

topology of the network, which may be because of battery fatigue or sometimes due to node mobility.

Yet different wireless networks exist that have both of these issues, for example, wireless ad-hoc networks. In these networks, wireless medium is used as communication channel, and they work with little infrastructure or none by any means. Various cryptographic procedures have been proposed to secure information transmission and intrusion detection in these networks [27], [28], [29], [30]. Such schemes are a blend of a few methodologies, including utilization of participating mobile nodes [31], [32], possibly combined with the analysis of audit logs [33], a game-theoretic approach [34], and various others.

However, the principle issue with most IoT devices lie somewhere else: in their constrained computational and communication assets and Internet Engineering Task Force (IETF) has categorized resource constrained devices into different classes [35]. IoT needs to work autonomously for longer period of times, and they need to run on on-board battery power. To meet these objectives, the energy utilization of IoT nodes must be minimized; this requires both the power productivity of the hardware, proficiency of communication standards, software that executes those standards and the security protocols used for information safeguard. The processing subsystem is perpetually realized using a small microcontroller with constrained resources, which runs at low clock rates, and in this way offers just unobtrusive computational and memory capabilities. Accordingly, the processing power of such subsystems is generally inadequate to run a full-scale software agent devoted to avert attacks.

A. Security Considerations

Security considerations in Internet of Things depend upon the need to identify what we are going to secure. The security contemplations [36][37][38][39] of IoT can be categorized as below:

*1) Data Confidentiality:*Confidentiality or privacy of information interchanges keeps away illegitimate users from learning message contents. To that end, we can utilize standard encryption methods which may incorporate secret keys shared among the communicating parties. But, encryption itself is not adequate for securing the information, because an eavesdropper can perform traffic examination on the overhead cipher text, and this can cause sensitive data to be leaked away. However, using encryption, protection of sensed information also needs to be implemented through access control mechanisms at the gateway to avoid misuse of information.

2) Data Integrity: Data Integrity in IoT is required to guarantee the fidelity of the information and alludes to the capacity to affirm that a message has not been messed with, modified or changed [40]. Regardless of the fact that the network has secrecy measures, there is still a great chance that the data integrity has been traded-off by modifications. The integrity of the network will be in danger when:

- A malevolent node in the network infuses false information.
- Unstable conditions because of wireless channel creating harm or loss of information.

3) Data Authentication: Authentication guarantees the trustworthiness of the message by recognizing its cause. An assault in IoT doesn't simply include the modification of packets; attacker can likewise infuse extra false packets [41]. Information authentication checks the identity of senders and receivers. Data authentication is realized through symmetric or asymmetric methods where sending and accepting nodes share secret keys. Because of the communication medium being wireless, it is a significant challenge to guarantee authentication [42].

4) Data Availability: Availability obliges that the IoT is functional throughout its lifetime. Denial of Service (DoS) assaults brings about a loss of availability of a network node. Practically, loss of accessibility may have severe effects. In a battlefield reconnaissance application, loss of availability may open a secondary passage for adversary intrusion. Different assaults can trade-off the accessibility of IoT. When considering availability in IoT, it is imperative to achieve graceful degradation in the existence of node compromise or benign node failures.

B. Security Threats

Illustrated below are the four classes of threats identified by P. Fleeger [43], that are likely to exploit the susceptibility of our security objectives and is shown in Figure 2 below.

1) Interruption: This type of security threat results in the loss of communication link between IoT devices. Malicious code addition, message corruption and node capture are among the few examples.

2) Interception: An unauthorized access has been gained and hence the IoT has been compromised by an attacker.

3) Modification: An adversary gains an unauthorized access to the data and tempers with it at the same time. For instance, modification of the data packets that are being transmitted resulting in the DOS (Denial of Service) attack, such as network flooding with bogus data.

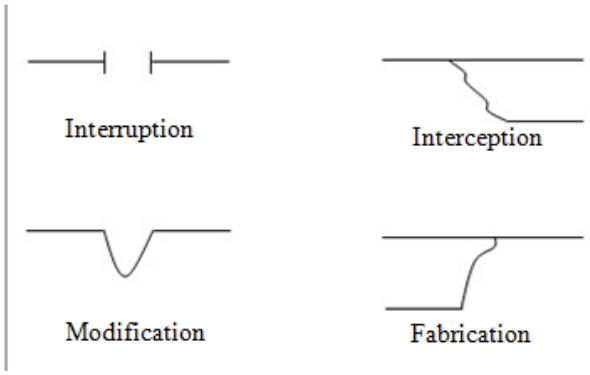

Figure 2. Threats Classification

4) Fabrication: Trustworthiness of the information is affected due to the injection of false data by the adversary.

3. Classification of IoT Security Attacks

The medium of communication and the resource constrained nature of IoT devices put them on a vulnerable track for potential security threats. Furthermore, the design of routing protocols for these kinds of networks does not usually address security issues. Therefore, attacks on such type of networks have maximum possibility to occur. In this paper, the potential attacks in IoT are categorized on the basis of security goal (CIAA) being exploited by them. Various types of possible attacks [44][45][46][47][48][49][50][51][52][53][54] on the control information and the transmission of data in IoT are defined below [55]:

TABLE 1. CLASSIFICATION OF IoT ATTACKS

Data Confidentiality Attacks	Data Integrity Attacks	Data Authentication Attacks	Availability Attacks
Sinkhole Attack	Data integrity attack	Blackhole attack	Homing Attack
		Spoofed, altered, or replayed routing information	Energy drain attack
Node replication attack	Man-in-the-middle attacks	Selective forwarding attack	Denial of Service attack
		Sybil attack	
Cold boot attack		Node replication attack	

A. Sinkhole Attack

A sinkhole attack is carried out by attracting all the traffic towards a specific node. The adversary tries to attract all the traffic from a specific area by making the use of a compromised node. It works by transforming a particular node appears attractive to the adjacent nodes[56].

B. Blackhole Attack

A node is placed in the range of the gateway in the Black-hole attack. This node promotes itself as the shortest route and draws all the traffic towards itself. Packets coming from a particular source within the network are dropped by the adversary. Because of this attack, certain nodes are isolated from the gateway resulting in the discontinuity in the network. This attack is easier to detect. Flooding based protocols are normally targeted using Black-hole attack.

C. Homing Attack

A kind of Black-hole attack in which the adversary keeps an eye on the network traffic and tries to deduce the location of some of the critical nodes[55]. These nodes can be disabled physically afterwards. The attacker can block the communication with the gateway so as to deliver a better ground to carry another attack such as sniffing or data integrity attacks. Malicious nodes should be prevented to join the network in order to prevent such attacks which can be achieved by implementing an efficient authentication protocol in IoT.

D. Spoofed, altered, or replayed routing information

One of the most common direct attack against any routing protocol is to alter routing information. The routing information that is exchanged between the nodes is a primary target. Adversaries might be able to repel or attract network traffic, generate routing loops, shorten or extend source routes, partition the network, generate pseudo error messages, and may enhance end-to-end latency. The standard resolution for such type of attack is to use authentication protocols i.e., routers should receive routing information from authentic routers exclusively [55].

E. Selective Forwarding Attack

Data gathering protocols in IoT mostly prefer multi-hop mode of communication. It is presumed in the multi-hop networks that the participating nodes shall be transmitting or receiving the information faithfully. However, the message may be refused to be forwarded by a malicious node and just drops the message, confirming that the information is not transmitted any further. Packet sequence numbers should be checked continuously in a conjunction-free network, so as to prevent such type of attack. Adding data packet sequence number to the packet header may help reducing selective forwarding attack [55].

F. Sybil Attack

Nodes possess some unique identity in the network. That's what is assumed by most of the protocols. An attacker makes himself seem to be at several positions at

the point of time while performing Sybil attack. This is achieved by creating a false identity of those nodes located on the edge of the communication range. The identity of authentic nodes is stolen or fabricated and hence multiple identities of nodes are occupied within IoT. A significant threat is posed by the Sybil attack towards the geographical routing protocols. Location aware routing regularly implicates nodes to interchange coordinate details with their neighboring nodes so as to construct the network. Therefore it presumes nodes to be present by means of a single set of coordinates , however making the use of Sybil attack, an adversary may be able to ‘‘be present at more places at the same time’’. Since the identity theft leads to this type of attack, appropriate authentication may be able to prohibit it [55].

G. Energy Drain Attack

IoT is organized dynamically and are battery powered. Replacing or recharging batteries is totally out of question and we want them to be functional as long as possible, as they are generally installed at those places where battery replacement becomes difficult. Fabricated reports generated by compromised nodes cause false alarms that lead to exchange of messages among legitimate nodes hence draining out a finite energy amount from the batteries powering the network. However, an adversary may only be able to carry out the attack, if his node possesses a sufficient amount of energy to transmit data packets constantly. The purpose is to destroy the legitimate nodes of the network, downgrade its performance and finally fragment the network grid. Adversary then takes control of the part of the fragmented network by the insertion of a new gateway node. To reduce the mutilation instigated by this attack, fabricated reports must be released en-route as soon as possible.

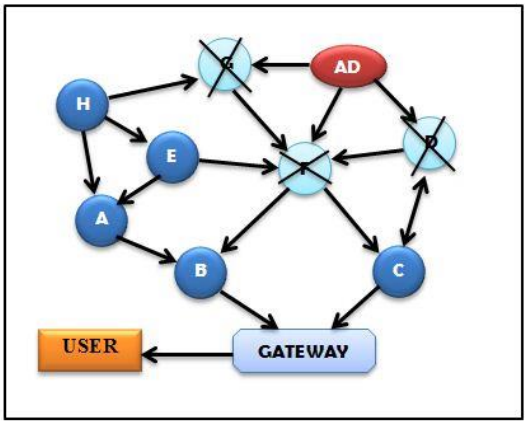

Figure 3. Energy Drain Attack

In figure 3, adversary node ‘AD’ generates false data constantly. The immediate neighbor nodes ‘D’,’F’ and ‘G’ respond to ‘AD’ and ultimately drains out their battery.

H. Denial of Service Attack

DoS (Denial of Service) attack is created by the adversary to overloading the network with bogus messages or even sending false data to IoT nodes so as to make the network resources unavailable. DoS attacks are not only meant for the attacker’s effort to destabilize, disrupt, or terminate a network, but for any occurrence that weakens a network’s capability to deliver a service. In IoT, various types of DoS attacks at different layers could be performed. At physical layer, the result of DoS attack could be tampering and jamming. At network layer, it may result in neglect and greed, misdirection, homing, black holes. For instance, if DoS attack cuts down serving node in IoT network, the other nodes that rely on this serving node functionally, will also be choked from serving their own client IoT nodes, therefore causing disruption in the entire network [57]. The mechanisms that are used to prevent DoS attacks comprise of payment for the network resources, secure authentication and traffic identification [42].

I. Main In The Middle Attack

In this type of attack, the adversary intervenes between the two communicating IoT nodes, accessing information, violating the secrecy of nodes by observing, snooping and controlling the information exchange between IoT nodes [58]. In Man-In-the-Middle attack, the assailant does not need to be physically there to launch the attack, but it relies on the network communication protocols of an IoT system.

J. Data Integrity Attack

Data integrity attacks trade off the information going among the nodes in IoT by altering the data contained inside the packets or infusing false data. An adversary node should have much more processing capabilities, memory and energy than the other legitimate IoT nodes[55].The objective of this attack is to misrepresent sensed data and thus compromise the integrity of exchanged information. It can also misrepresent routing information to disturb the network’s routine operation, potentially making it futile. This is also considered to be a kind of denial of service (DoS) attack. This attack can be protected through the adaption of asymmetric key system, which is used for encryption and\or digital signatures, but involves much of additional overhead to IoT nodes.

K. Node Replication Attack

In this type of attack, an adversary attempts to install a number of nodes having similar identity at various locations of the existing IoT network. There are two techniques for launching node replication attack. In the first technique, the adversary captures a node from the target network and produces a clone of the captured IoT node and places it at different locations within the

network. In the second technique, an attacker could produce a pseudo-identification of an IoT node, creates a clone out of this node and then places it at different locations within the network. These clones try to generate fabricated data in order to disrupt the network. Node replication attack is quite different from that of the Sybil attack. In Sybil attack, many identities of a single node are present in the network, but in node replication attack, different nodes are present with the same identity. Hence, in Sybil attack an attacker has high chances to succeed by placing just one node, whereas in node replication attack it needs more nodes to be installed throughout the network which maximizes detection rate. This attack can be avoided by validating the identities (authentication) of nodes by a node which is trustworthy.

L. Cold Boot attack

It is a type of side channel attack where an adversary gets unauthorized access of IoT node and then obtains encryption keys when the node is left unattended. It is also known as platform reset attack. After intruder gets encryption keys, the privacy of messages is compromised and intruder can then launch malicious attacks.

4. EXISTING SECURITY PROTOCOLS

Recently, IoT security has possessed the capacity to pull in the attentions of various researchers around the globe. A broad variety of security protocols have been suggested for resource constrained networks like wireless sensor networks to deal with malicious attacks. These protocols can be implemented for Internet of Things as IoT also falls in limited resource networks. In this section, different security protocols proposed for IoT and other suitable protocols for Internet of Things will be presented with advantages and drawbacks of each scheme.

A. Existing Protocols

Attribute Based Encryption (ABE) scheme is used in [59] to safeguard the information exchange for Publish-Subscribe (Pub-Sub) architecture based IoT. In this scheme, Advance Encryption System (AES) cryptography is used to encrypt payload and ABE scheme is used to encrypt AES key itself. As is already known that IoT devices have restricted resources and create lesser number of bits of data. Hence, to encrypt these small chunks of data using AES and ABE cryptographic techniques is not suitable for IoT as these involve complex arithmetic operations.

Xiong Li, et al. [60] proposed trusted security architecture for IoT. However, the proposed system uses complex algorithms at each layer which makes it unsuitable for limited power components like sensors and RFID which are regarded as skeleton for IoT. A hybrid encryption technique is proposed in [61] for safeguarding the data in IoT devices. The cryptographic methods used in this technique include Advanced Encryption System (AES) and Elliptic Curve Cryptography (ECC), but these methods are highly complex and drain off the limited battery of nodes rapidly and thus unsuitable for IoT. Do et al. [62] and Li et al. [63] have reported that design flaws and vulnerabilities of softwares and systems in Internet of Things need to be assessed frequently so as to improve the cryptographic schemes timely in IoT.

B. Suitable Protocols

1) MiniSec: This protocol is primarily implemented to secure the network layer[64]. Power constraint forces IoTs to consume energy in an intelligent manner. This protocol provides reasonable security without consuming much of the constrained energy available at IoT devices. This protocol was designed to provide security to wireless sensor network and specifically for Telos sensor motes. It possesses two functional approaches viz broadcast multi-source communication known as Broadcast (Minisec B) and single-source based communication known as Unicsat (Minisec U), both utilizing Offset Code Book (OCB) approach to provide authentic encryption. The functionality of OCB scheme is as follows:

Let us suppose that M is a message of variable size and it requires to be encrypted and H is an ordinary message header. Both M and H require authentication, where K acts as the encryption-key and N is a non-repeating value. It is going to be considered as birthday attack if the value of N is repeated. Initially, OCB takes M, K, N and generates cipher text core C. and at the time it uses M plaintext message, C, H and generates a tag of length τ. The final output of *OCBK* (*N, M, H*) is the tuple (*Ctag*) [48]. In order to decrypt this encrypted message at the receiver's end, receiver should perform the reverse process. Unicast goes for single-node communication while as Broadcast utilizes multicasting or broadcasting group of nodes.

Low energy consumption and high security are the characteristics of this protocol that are publicly available in their implemented form. However, this protocol consumes more energy when large data packets are transmitted by Radio Frequency (RF) which is considered as drawback of this security protocol.

2) SPINS: SPINS (Security Protocol for Information via Negotiation protocol) is used to secure the communication links from active and passive threats offering two sets of protocols, "SNEP and µTESLA [65]".

SNEP (Secure Network Encryption Protocol) is employed for two-party data authentication, data-confidentiality and data-integrity, while as, µTESLA

(Micro Timed Efficient Stream Loss tolerant Authentication) is conscientious for authenticated broadcast. Both of these security variants of SPINS utilize symmetric encryption algorithms.

SNEP offers secure end-to-end communication through the policy of focusing upon data confidentiality, integrity, two-party data authentication, replay protection and weak-message freshness. On the other hand, µTESLA assures the sharing of information securely without any tampering by an attacker throughout broadcast communication process.

This protocol delivers best security, lesser communication overhead and easy to be implemented. However, it suffers from the flaws of having minimal power management. The drawback of SPIN protocol is that it is not certain about the data being delivered to the target as a result of tampering by adversaries. In a scenario where the target node wants to get data from far away source node and the surrounding nodes are not interested in that data, such type of data will remain totally undelivered. Therefore, SPIN is surely not a wise choice for applications [66]. This protocol makes use of symmetric approach for encryption and decryption, while asymmetric approach is used for key distribution. This approach does not provide adequate security due to resource constraints and requires a long battery life.

3) Localized Encryption and Authentication Protocol (LEAP): Zhu et al. proposed LEAP as a key management protocol for sensor networks [67]. LEAP utilizes four types of keys for every node and communication type, they are: "an individual key shared with gateway, a pairwise key shared with other IoT node, a cluster key imparted to different neighboring nodes, and a group key that is shared by all IoT nodes" [68].

In individual key sharing, every node has allotted a unique key that is shared with pairwise to the gateway for secure communication between gateway and node. In Pairwise key sharing, each node distributes its pairwise key with neighboring nodes. This pairwise key is used for privacy and source authentication. Cluster key is shared with every node and the purpose of this key is to secure the message broadcast locally. Group keys are globally defined and are used between gateway and group member nodes.

The primary advantage of LEAP is that it resolves the issue of key distribution among nodes and confines the effect of compromised node to the network. However, the numerous messages that must be exchanged during the establishment of keys, which result in increased communication cost and energy utilization is a big drawback of this protocol.

*4) Neighborhood based Key Agreement Protocol (NEKAP):*It is a key management protocol that creates two types of keys: pairwise keys, for pairwise communication and cluster keys, for broadcast communication [68]. It is identical to LEAP, however NEKAP is stronger against node tampering and is considerably more energy efficient. In NEKAP, each node is preloaded with a master key, encrypted by a global shared key, which is then broadcasted to adjacent nodes. The master keys of neighboring nodes are used to create a node key which makes it difficult for the intruder to get the value of key. Each node broadcasts just three messages to set up all key therefore, making this protocol energy proficient.

The main advantage of NEKAP is that the effect of compromised node is confined to that node's vicinity as each key is valid only in its neighborhood. Therefore, it is difficult for an intruder to perform wide-scale attack by trapping just a couple of nodes. Additionally, the energy expense of this mechanism is lower than that of past methods. NEKAP has numerous benefits on the grounds that it is adversary resilient and energy proficient.

Unluckily, NEKAP is susceptible to replay assaults [69] due to key set up process. A malevolent node may send out an old message that was initially broadcasted from an authorized node to its adjacent nodes, and the message can't be authenticated in light of the fact that these two nodes can't communicate directly. Subsequently, a malignant node may gain legitimate status by deceiving the chosen authorized nodes by transmitting an old message, and after that the intruder may initiate different assaults, such as DOS assaults, black hole assaults, or masquerade assaults.

Furthermore, both LEAP and NEKAP are experiencing node tampering amid network instatement. Since NEKAP includes the establishment of keys among nodes and subsequently various communicative messages are to be interchanged which lessens node lifetime by an impressive time as 80% of node energy is utilized for communication related tasks.

5) Energy Efficient and Dynamic Security Protocol (EEDSP): This scheme has proved to be energy efficient for wireless sensor networks as it uses the limited available energy of nodes efficiently. In this scheme, the data at sensor nodes is encrypted by dynamically generated key. Repeated encryption and decryption cycles are performed periodically to make the information secure at nodes. This scheme provides security to data in-transit and also, when the data is left

unattended at sensort nodes by following the encryption-decryption cycles with different dynamically generated keys [70].

C. Suggestive methods (Proposals) to improve IoT security

1) Proposal for Key Management: Symmetric cryptographic protocols are suitable to be used in ressource constrained Internet of Things nodes in comparison to assymetric protocols. But one of the main issue with symmetric key cryptographic protocols is with key management i.e. how the key is shared between communicating nodes. Cryptographic keys must be negotiated and periodically refreshed in order to gaurantee effective security. Therefore, new lightweight key management methods suitable for Internet of Things may be designed.

2) Proposal for Routing Protocol security: Internet of Things employ RPL as routing protocol that defines mechanism to protect routing control messages, however, no further security mechanisms are developed in the current version of RPL standard [14]. Considering that RPL provides mechanisms to secure routing communication against external attacks, research efforts may focus on developing security mechanisms to safegaurd RPL communications from internal attacks where the attacker is in possession of IoT node and may inject false routing messages.

5. CONCLUSION

Internet of Things is proving to be of extreme importance to the computing society as an outcome of its various applications including observing the physical and environmental conditions, surveillance purposes, supply chain management, defense applications, smart buildings, disaster alerts, smart homes, smart cities, and so on, where conventional networks are not ideal. To enable the growth of IoT at its full pace, one of the main obstructions is to provide security and privacy to the communicating messages in IoT network.

In this paper, we have classified the possible attacks in IoT based on their impact on the type of security goal being compromised. We have also surveyed the literature on the existing security methods for IoT and other related fields, and also summarized the limitations and benefits of each of the security method from which several conclusions can be drawn. One can conclude that security is expensive in terms of memory and computations. It is generally easy to implement complex security algorithms for powerful resource-rich devices but the same is not the case with IoT that brings new challenges. The constrained resources do not permit to execute existing solutions inminiature devices like IoT with several limitations. The focus in a security scheme for IoT is to maximize security of information, reduce the impact of attacks and have less energy consumption in the process. The privacy and security issues for resource constrained IoT devices need to be addressed and implemented immediately, so that IoT can be put to work with its full potential. In this direction, we have provided possible research opportunities for future research work.This survey will hopefully motivate future researchers to come up with smarter, energy efficient and more robust security protocols and make IoT safer.

REFERENCES

[1] V. Marcos and S. Diogenes, “Survey on Wireless Sensor Network Devices,” Technical report IEEE-0-7803-7937/03, Federal University of Minas Gerais,2003.

[2] D. Singh, G. Tripathi, and A.J. Jara, "A survey of Internet-of-things: Future vision, architecture, challenges and services," In Internet of Things (WF-IoT), IEEE World Forum, pp. 287-292,2014.

[3] Y. Chen and Nasser, “Enabling QoS multipath routing protocol for wireless sensor networks,” in IEEE International Conference, pp. 2421 – 2425, 2008.

[4] D. Evans,“The Internet of Things: How the Next Evolution of the Internet isChanging Everything”, CISCO white paper, 1, 2011.

[5] D. Surie, O. Laguionie, and T. Pederson,“Wireless Sensor Networking of Everyday Objects in a Smart Home Environment”,IEEE International Conference on Intelligent Sensors, Sensor Networks, and Information Processing, pages189–194, 2008.

[6] H. Alemdar and C. Ersoy,“Wireless Sensor Networks for Healthcare: A Survey”, Computer Networks, 54(15), pp. 2688 – 2710, 2010.

[7] S. Li, L. Xu and S. Zhao, “The internet of Things: A Survey”, Information System Frontiers, Springer, Volume 17, Issue 2, pp. 243–259, 2015.

[8] L. Milić and L. Jelenković, "A novel versatile architecture for Internet of Things," International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, pp. 1026-1031., 2015.

[9] IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LRWPANs), IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006), (2011) 1-314.

[10] IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)Amendment 1: MAC sublayer, IEEE Std 802.15.4e-2012(Amendment to IEEE Std 802.15.4-2011), (2011) 1-225 .

[11] ZigBee Alliance, ZigBee specification, 344-346, 2006.

[12] The International Society of Automation, Wireless Systems for Industrial Automation: Process Control and RelatedApplications ISA 100.11a, 2009.

[13] Kim A. et al., “When HART goes wireless: Understanding and implementing the WirelessHART standard”, IEEE InternationalConference on Emerging Technologies and Factory Automation,ETFA 2008.

[14] Thubert P. et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, 2012.

[15] C. Bormann, A. Castellani, Z.Shelby, "CoAP: An Application Protocol for Billions of Tiny Internet Nodes", IEEE InternetComputing, 1 (2), pp. 62-67, 2012.

[16] D. Locke, "MQ Telemetry Transport (MQTT) V3.1 Protocol Specification, " http://www.ibm.com/developerworks/library/ws-mqtt/, 2010.

[17] Standard OASIS, Oasis advanced message queuing protocol (amqp) version 1.0. 2012 http://docs.Oasis-open.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os. Pdf.

[18] http://www.omg.org/spec/DDS/1.4/PDF/.

[19] A. Ahmed, H. Shi and Y. Shang. "A survey on network protocols for wireless sensor networks," Proceedings of Information Technology: Research and Education, , pp. 301-305, 2003.

[20] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebeke, F. V. Abeele, E. D. Poorter, I. Moerman and P. Demeester, IETF standardization in the field of Internet of Things (IoT) A survey, Journal of Sensor and Actuator Networks, Vol. 2, pp. 235-287, 2013.

[21] Keynote ADCOM, 2014. Retrieved from http://www:cse:wustl:edu= jain=talks=iotad14:htm:

[22] A. Jules, "RFID security and privacy: a research survey", IEEE journal onselected areas in communications 24 (2), pp. 381-394, 2006.

[23] J. Bukley, "From RFID to the internet of Things: final report", In EuropeanCommission Conference,Brussels, Belgium, March, 2006.

[24] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey",Computer Networks, Vol. 54, no. 15, pp. 2787-2805, 2010.

[25] M. N. Elshakankiri, M. N. Moustafa and Y. H. Dakroury. "Energy Efficient Routing Protocol for Wireless Sensor Networks," International Conference on Intelligent Sensors, Sensor Networks and Information Processing, pp. 393 – 398, 2008.

[26] Q. Zhou, M. Elbadry, F. Ye, Y. Yang, "Flexible, Fine Grained Access Control for Internet of Things", IoTDI'17- ACM, Pittsburgh, PA, USA, 2017.

[27] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks", In SAINT: Symposium on Applications and the Internet, pp. 368-373, 2003.

[28] A. Mishra, K. Nadkarni, and A. Patcha. "Intrusion Detection in Wireless Ad-hoc Networks", IEEE Wireless Communications, Vol. 11, No. 1, pp. 48, 2004.

[29] Y. Zhang and W. Lee,"Intrusion detection in wireless ad-hoc networks",MobiCom: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 275-283. ACM Press, 2000.

[30] Y. Zhang, W. Lee, and Y.-A Huang,"Intrusion Detection Techniques for Mobile Wireless Networks", Wireless Networks, Vol. 9, pp. 545-556, 2003.

[31] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong,"Decentralized intrusion detection in wireless sensor networks",Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, pp. 16{23, 2005.

[32] C. Kruegel,"Applying mobile agent technology to intrusion detection in Distributed Systems Group", Technical University of Vienna, 2002.

[33] O. Kachirski and R. K. Guha, intrusion detection using multiple sensors in wireless ad hoc networks. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences, pages 57-65, 2003.

[34] A. Agah, S. K. Das, K. Basu, and M. Asadi,"A non-cooperative game approach for intrusion detection in sensor networks",IEEE International Symposium on Network Computing and Applications, pp. 343-346, 2004.

[35] C. Bormann, M. Ersue, and A. Keranen,"Terminology for Constrained-Node Networks", .RFC 7228, IETF, 2014.

[36] E. Yoneki andJ. Bacon, "A survey of Wireless Sensor Network technologies: research trends and middleware's role", technicalreport. http://www.cl.cam.ac.uk/TechReports,2005.

[37] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security - a survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRCPress, 2007.

[38] L. Fernandes, "Introduction to Wireless Sensor Networks Report", University of Trento. http://dit.unitn.it/~fernand/downloads/iwsn.pdf, 2007.

[39] T. A. Zia, "A Security Framework for Wireless Sensor Networks". http://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pdf, 2008.

[40] P.Bansal, B.Yadav, S. Gill, H.Verma, "Security Attacks in Wireless Sensor Network", International Journal of Scientific & Engineering Research, Volume 3, Issue 4, 2012.

[41] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of SecurityIssues in Wireless Sensor Networks," IEEE Commun. SurveysTutorials, vol. 8, pp. 2–23, 2006.

[42] G. Padmavathi, D. Shanmugapriya," A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[43] C.P. Fleeger, "Security in computing", 3rd edition, Prentice-Hall Inc. NJ, 2003.

[44] S. Kaplantzis, "Security Models for Wireless Sensor Networks", http://members.iinet.com.au/~souvla/transferfinal-rev.pdf, 2006.

[45] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for Self-Organization of a Wireless Sensor Network", IEEE Personal Communications, pp. 16-27, 2000.

[46] A. Woo and D. Culler"A Transmission Control Scheme for Media Access in Sensor Networks", Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking,Italy, 2001.

[47] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, andA. Chandrakasan, "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks", Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, pp. 272-287, 2001.

[48] C. Shen, C.Srisatjapornphat, and C. Jaikaeo, "Sensor Information Networking Architecture and Applications",IEEE Pers. Communication, pp. 52–59, 2001.

[49] Committee on National Security Systems(CNSS), National Information Assurance Glossary, NSTISSI,No.4009.http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf, 2006.

[50] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks",IEEE Computer, 35(10), pp. 54-62, 2002.

[51] L. L. Fernandes,"Introduction to Wireless Sensor Networks Report", University of Trento.http://dit.unitn.it/~fernand/downloads/iwsn.pdf, 2007.

[52] I. Siahaan and L. Fernandes, "Secure Routing in Wireless Sensor Networks", University of Trento. http://dit.unitn.it/~fernand/downloads/IWSNSlides.pdf, 2008.

[53] A. Dimitrievski, B. Stojkoska, Trivodaliev,D. K.andDavcev, "Securing communication in WSN trough use of cryptography", NATO-ARW, Suceava, 2006.

[54] B. Parno, A. Perrigand V. Gligor "Distributed Detection of Node Replication Attacks in Sensor Networks", Proceedings of the IEEE Symposium on Security and Privacy, 2005.

[55] P.Mohanty, S. Panigrahi, N. Sarma and S. Sankar, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, 2005.

[56] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad-hoc Networks (elsevier), pp. 299-302, 2003.

[57] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena and M. S. Obaidat, "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things," IEEE International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, pp. 114-122, 2011.

[58] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges," International Journal of Computer Science and Information Technology & Security vol. 1,no. 2, pp. 136-146, 2011.

[59] X. Wang, J. Zhang, E. M. Schooler and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," IEEE International Conference on Communications (ICC), Sydney, NSW, pp. 725-730, 2014.

[60] X. Li, Z. Xuan and L. Wen, "Research on the Architecture of Trusted Security System Based on the Internet of Things," IEEE International Conference on Intelligent Computation Technology and Automation, Shenzhen, Guangdong, pp. 1172-1175, 2011.

[61] M Xin, "A Mixed Encryption Algorithm used in Internet of Things Security Transformation System," IEEE International conference on cyber-enabled distributed computing and Knowledge Discovery, 2015.

[62] Q. Do, B. Martini and K. K. R. Choo, "A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2174-2186, 2016.

[63] B. Li, R. Lu, W. Wang and K. K. R. Choo, "DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2415-2425, Nov. 2016.

[64] M. Luk, G. Mezzour, A. Perrig and V. Gligor, "MiniSec: A Secure Sensor Network Communication Architecture", ACM 978-1-59593- 638-7/07/0004IPSN'07, 2007.

[65] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", ACM, 2001.

[66] N. Rathi, J.Saraswat, P. Bhattacharya, "A Review On Routing Protocols For Application In Wireless Sensor Networks", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.5, 2012.

[67] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", SenSys'03, ACM 1-58113-707-9/03/0011, 2003.

[68] D. Zhang, Y. Zhao, X. Wang, J. Choi, "A Robust and Efficient Neighborhood-Based Security Protocol for Wireless Sensor Networks", International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2010.

[69] M. Vella and A.Mahdy, "Survey of wireless sensor network security", National Conference for the Society for Advancement of Chicanos and Native Americans, Salt Lake, Utah, USA, 2008.

[70] A. Bashir and A. H. Mir, "An energy efficient and dynamic security protocol for wireless sensor network," International Conference on Advanced Electronic Systems (ICAES), Pilani, pp. 257-261, 2013.

Adil Bashir received his Bachelor of Technology (B.Tech) in Computer Science and Engineering from Islamic University of Science and Technology, Jammu & Kashmir, India in year 2011. He has done his Master of Technology (M.Tech) in Communication and Information Technology from National Institute of Technology (NIT) Srinagar, India in 2013. Presently he is a research scholar at NIT Srinagar in the Department of Electronics and Communication. His research interests are Internet of Things, Wireless Sensor Networks, Embedded Systems and Network Security.

Ajaz Hussain Mir has done his Bachelor of Engineering (B.E) in Electrical Engineering with specialization in Electronics & Communication Engineering (ECE). He did his Master of Technology (M.Tech) in Computer Technology and PhD both from IIT Delhi in the year 1989 and 1996 respectively. He is Chief Investigator of Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA).

Presently, he is Professor in the Department of Electronics & Communication Engineering at NIT Srinagar, India. He has been guiding PhD and M.Tech thesis in Security and other related areas and has a number of International publications to his credit. His areas of interest are Biometrics, Image processing, Security, Wireless Communication and Networks.