International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Security Issues and Challenges in IoT Routing over Wireless Communication

G. Saibabu, Anuj Jain, V. K. Sharma

Abstract: ***The participation of Internet devices in different communications through embedded technologies and the adaptive and interactive nature of each communication affects future development tools and applications. The majority of IoT devices are able to communicate over a wireless network, improving their usability and scalability quickly. But these usability improvements drew the attackers' attention to their personal advantages and created numerous security challenges for detection and protection. Because devices are exposed to the Internet to deliver services, they are particularly vulnerable to various threats to security and privacy.Therefore, a major concern on the Internet of Things (IoT) is the discovery of such abnormal activities that pose a security threat so that appropriate solutions can be provided with a high level of reliability. This paper will be based on a detailed overview of IoT wireless security issues and abnormal activity detection methods. It also provided an overview of the various anomaly detection models and security challenges for launching the IoT connection to the wireless network.***

Keywords:Internet of Things, Security, Challenges, Anomaly Detection, Wireless Sensor Network.

I. INTRODUCTION

In recent years, the Internet of Things (IoT) has gained tremendous room for development in communications infrastructure to integrate computers into the Internet. The prospects in the field of computers and wireless mobile phones have increased research and industrial interest. The IoT can interpret any type of complex, intelligent old sensor that affects the development of new applications, allowing resources to be exchanged locally or globally. IoT devices and related applications are used to quickly detect and transmit data in many areas, such as "hospitals", "energy monitoring", "live", "agriculture", "military", etc. Data and services [1], as shown in Fig.1. In addition to many benefits, its main focus is privacy, unauthorized access, and security attacks that can cause many unusual activities, such as Internet exposure. These unnatural activities may cause the quality of IoT to decline and may cause problems in its future adaptation.

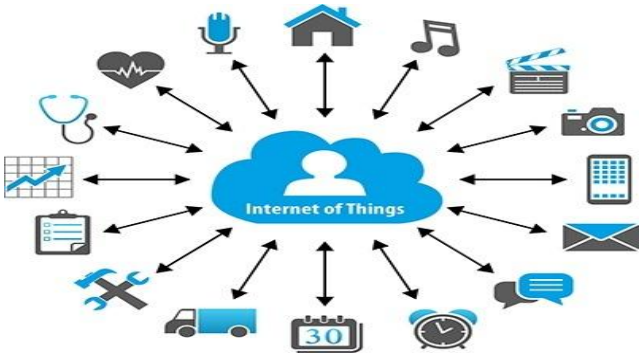

Fig. 1 Usage of IoT Application (Source: Internet)

According to Cisco's IoTvalue and trust survey among 3,000 consumers, [2] it reveals confidence in and adaptability to IoT services. The survey found that most consumers believe that IoT services can provide great value to their needs, but they do not understand how to solve the security of their data. This refers to the deep integration of consumers when using IoT services in their daily lives, without worry, uncertainty, and risk [3]. At least 9% of consumers believe that the data collected and shared via the IoT is safe, and all other consumers are still interested in how data is protected and utilized.

This global focus on IoT can be addressed by a security system to prevent anomalies based on anomalies and detect malicious attacks. Additionally, there are several other issues that must be addressed in Physical Communications and Networks pane. IoT applications typically have special requirements in real-time and are expected to be highly reliable and work in critical security environments. These requirements provide a very high level of security and confirmation.

IoT devices are limited in terms of memory, processing, and bandwidth. It will not be possible to establish a traditional security mechanism because it requires more memory and processing. For mobile IoT devices, frequent changes in network topology can also affect the management security system [4]. Therefore, it is difficult to implement a conventional security solution to provide the full security needed for security challenges. For this reason, it is important to have a lightweight system that effectively monitors the harmful activities that predict the security risks that hackers need to protect.

Anomaly detection (AD) [5], [6] is a simple monitoring process used by network hackers or various applications to detect fraud. It builds an assessment model based on retrospective observational behavior to classify the disorder class. The IoT device typically transmits all of its information to a centrally arranged site and facilitates event behavior analysis to effectively classify infiltrators. The rise of IoT diversity raises serious concerns about security and privacy.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Saibabu Gutta*, Pursuing Ph.D, Department of Electronics and Communication Engineering, Bhagwant University, Rajasthan, India.
Anuj Jain, Professor, Lovely Professional University, Punjab, India.
V. K. Sharma, Professor, Department of Electronics & Telecommunication Engineering, Maharashtra Academy of Engineering, Alandi, under Pune University, India.

Wireless Sensor Network (WSN) is the interconnection of low-power devices by means of wireless protocols, and IoT is a concept that connects WSN and the Internet to expand worldwide [3], [7]. IoT devices are interconnected by a medium based on wireless Internet technology sensors and actuators (called things), and these interconnections grow into a wide network or a group of networked devices. The statistics are shown in the statistics portal [8] (Fig. 2) show that the number of connected IoT devices worldwide increased by 31 billion between 2015 and 2025.

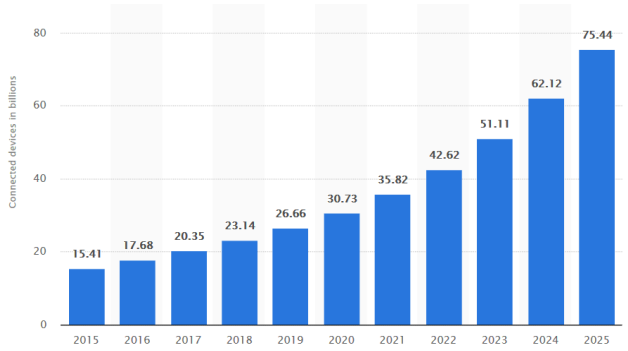

Fig.2. A forecast of IoT connecting device worldwide from 2015 to 2025 (Statista, 2016)

The increased use of IoT devices between people requires a secure, high-quality connection between interactive devices. As the analysis in Figure 2 indicates, the IoT will grow significantly in the future, and it must have a strong security framework to maintain the privacy of services. In reviewing past issues and concerns about IoT devices, we aim to address the importance of security issues in IoT-based security systems to address the importance of threats or attacks in this survey. It focuses on key security issues in data routing and anomalous forecasting to understand the nature of routing events and identify anomalies in IoT security systems.

In the following papers, Section-2 discusses security issues and challenges in WSN, Section-3 describes security methods in WSN, Section-4 discusses IoT security analysis, and Section 5 discusses IoT. safety. Importance of Secure Routing In the IoT, Section-6 discusses security constraints and openness issues and Section-7 presents the conclusion of the survey.

II. SECURITY ISSUES AND CHALLENGES OF WSN

Ensuring the security of the WSN is critical, so there is a large body of literature on detecting and mitigating attacks against such networks [9], [10]. Depending on the type of attack, follow different strategies and algorithms.

The existing AD model has adopted three types of structures: "local", "centralized" and "distributed". In the limitedconstruction, the anomaly identifier is applied to the node range without the cooperation between the nodes in the network. In a centralized architecture, the entire data is transmitted to a central place where AD operations are performed, such as a base station or cluster head. Ultimately, the distributed constitution employs associationamong nodes in the identifier process, where every node transmits a data digest characterized by the cluster's confined natural mention model to construct a generic global reference model [6], [11]. Each node in the cluster then uses the global reference model for subsequent testing.

Therefore, distributed discovery is best to reduce power consumption. At the same time, the size of the local generic reference form sent to the cluster header should be a small digest size to decrease communication overhead. An additionalfeature to consider in a distributed architecture is the number of times the confinedmention model has to be transmitted to the team organizer, so the frequency of the global reference model of the local mention model oughttobereformed. The current IoT sensor network infrastructure provides direct physical access through "manipulation" and "denial of service."

2.1 Tampering

Tampering occurs when an attacker physically modifies a device or connector. This material layer provides a large attack surface. Access, theft or replacement of equipment items may infringeprivacy, accessibility and security objectives. In one directionitcaneliminatethroughutilize a tamper-proof system [12].But such systems can be very high-pricedfor the existence of inexpensive power sensors or consumer appliances that are the primary drivers for the IoT.

The tampering connectionsare in form of disconnecting or altering the physical link that is considered to be a "denial of service (DoS) attack" state or changing the broadcasting data to a "man in the middle attack" state [13]. On the other hand, if the vulnerability is manipulated, the IoT sensor poses a major security threat to the “DDoS attack” [10].

2.2 Denial of Service Attack

In generalsituations, Io Tappliances correspondviawireless access equipment in the physical layer. Wireless links are highly vulnerable to DoS attacks, which able toacquire the structure of signal alteration or interference. This attacksable to affect the system accessibility [14]. Although a wide range of spectrum technologies can be used to combat radio interference, there is no universal answer to elevatethese attacks. Even current methods needed a lot of processing, and these processes do not have the resources needed to limit the devices in the IoT. So, it needsprobableresolutionwhichcanobserve and understand traffic to provide solutions [15].

Many vulnerabilities can be exploited in routing protocols for sensor networks. Various countermeasures have been proposed to detect these attacks. In [16], lightweight systems use multiple location recognition techniques to trigger an alarm if an intermediate sensor does not respond. Each time the sensor receives a packet, it sends an ACK to the sensor to process the packet in the previous jump. If the sensor receives less than the ACK for a specified period of time, it is doubtful that the previous report it sent was dropped by the malicious sensor. In this case, an alert packet will be sent to the receiver, reporting the next transition sensor as a potential damage sensor.

The authors proposed a central approach using "SupportVectorMachines (SVM)" [17]. They were initially trained without an attacker, and the number of hops and measured bandwidth in the receiver was used as a feature. At run time, an SVM-based detection algorithm is applied to the receiver.

A different method is used in [18], where each sensor observes the behavior of its neighbors by recording the number of packets they send and the address of the original sensor source. Based on these observations, he updated the trust schedule for each neighbor to detect potential attackers. After the sensor is named an attacker, the routing table is modified to isolate the sensor from the network.

III. SECURITYAPPROACHES IN WSN

Security is the process that is performed on a data point to determine whether the data point is normal or abnormal. The AD method tries to find the basic distribution that determines the normal value, so you can say exactly when the data point does not follow the normal value. The above methods have shown that the greater the number of data points, the estimates are either biased [19] or unbiased [20]. It calculates deviations and differences, or at least provide an expression [21].

Some existing security solutions use a centralized approach that collects data from the sensor and transmits it completely for the cluster head or base station for processing.However, data transfer costs are several times higher than data processing costs. Furthermore, communication between sensor nodes is required to design a distributed AD model. Due to this, energy consumption is affected by the total amount of traffic produced by the delivery process of distribution.Because of the many challenges involved in creating AD in IoT security, some of the key security challenges are listed in the following summary.

3.1 Access Control

Access control handles access to objects/devices in an IoT environment. In a traditional database system, separate data is processed, but in the IoT, stream data is processed. Two terms of access control [22] are described as 1) Data carriers that send/receive data to objects. They must send the data to the authentication object, 2) the "data collector" that the user must authenticate. The authentication problem in data stream outsourcing was discovered in [23]. Data access control is specified in [22]. Some access control challenges in the IoT environment include how to handle large amounts of data transmitted in a recognized representation.

3.2. Privacy

Data labels are proposed to manage IoT privacy in [24]. Based on the anonymous identity privacy model in [25], the access control protocol and the user's privacy control are suggested. [24] Identify an anonymous model by changing the quasi identifier to maintain sensitive data. The privacy risks that occur when you assign a static domain name to the IoT node are identified in [25]. Some IoT privacy issues are covered only in modern businesses, and the scope for creating privacy mechanisms in the IoT environment remains high.

3.3. Trust

The concept of trust is used in different contexts and in different interpretations. Trust is a complex concept and there is no interpretative acceptance in the scientific literature [26]. In addition, its importance is determined in two dimensions. In many applications that describe trust, the basic problem is that they do not contribute to the representation of metrics and computational methods. Satisfying trust constraints is entirely related to the impact of identity negotiation and access control.

3.4. Authentication & Confidentiality

Different works describe different protocols and mechanisms for handling user authentication and data confidentiality in the IoT environment. The following are some of the key operations related to authentication and confidentiality in the IoT. In [27], the current IoT application protocol for business intelligence security combines cross-platform communication with encryption, signature, and authentication to provide improved IoT application development capabilities. In [23], the implementation of the security system defines two-way authentication in the IoT. Regarding confidentiality and integrity, in [28], how to apply the current key management system in the context of the IoT was studied. In [29], the PKI framework was designed for the IoT. All of this current work is based on solving lightweight encryption issues in the released environment. However, more work is needed to establish standardized authentication and confidentiality protocols to address current IoT security challenges.

IV. ANALYSIS OF IoTSECURITY MODELS

Insecurity, AD has been widely used in many applications [30], [31]. The majority of familiar methods are within the range of "statistics", "clustering", and "machine learning".Thesemethods are classified as "supervised", "semi-supervised" or "unsupervised", based on the nature of the process, it is required to sample the data.

Supervised technology requires training data with a label indicating each sample category. Then, it creates a new unspecified sample form the selected class. Semi-observational methodsneed the use of samples from a certain category to train the data to create a pattern of whether the new sample belongs to that category. Finally, uncontrolled techniques do not require specific training data, and data sets can be divided into different subgroups without the need for previously learned models [32].

H. Suo et al. [19] describeIoT stating that it derived from the term "Internet" and itsequivalentmethods, in related to the conventional "Internet", "mobile"and"sensor" networks, where all of these are associated to the Internet, and these equipment communicate with the other one. R. H. Weber [25]describethese types of schemes have immense flexibility and scalability perspective, but they also have security issues. There are many threats to adopting it, and no threats are raised without a major solution. This technology may not be feasible in the near future.

The IoT layer suffers from a variety of security threats identified in the computer network community. The following subsections provide an overview of cyber threats and attacks that can have a major effect on IoT systems.

4.1 Denial of Service attacks

1) *Spoofed routing Message*: Althoughpacket payload messageis encrypted on the routing channel, routing and earlier header messagesare not encrypted. The messagetransmitted in the routing protocol is usually the primary intention of spoofing.

An attacker could compromise network traffic by spoofing, changing or re-reading IP addresses or transport protocol messages. The outcomepossiblyarouting iteration, derived methods, faked error information, and so on [33].

2) *Selective forwarding*: In a multi-hop network, a malicious node may change or tamper with traffic by discarding certain messages to selectively redirect other messages. The information to the destination is incomplete and is therefore destroyed in some way. In this type of attack, malicious nodes do not selectively forward and discard certain messages to ensure they do not propagate in the future. An attacker mostlyaccountable for quenching or modifying packets initiating from several nodes is able to redirect the rest of the traffic to detect no violationsfor a moment. In this kind of attack, a disruptive node randomly bypasses certain messages [34].
3) *Sinkhole attack*: In this kind of attack, certain nodes or destinations are additionalstriking to traffic in other natural nodes. When accessing a streaming node, messages possibly will be dropped, messages may be routed using the changed content, or otherwise altered. This can lead to congestion and possibly speed up the powerutilization of the nodes engaged. Because the vulnerability is configured in the sensor network, it is susceptible to numerous other DoSattacks [11].
4) *Sybil attack*: The Sybil attacker type uses a node or multi-identity device. These produce traffic that looks like multiple sources or even distributed. This approach undermines the use of fairness, redundancy, or voting concepts that already exist in the infrastructure. This is shown as a malicious device that illegally acquires multiple identities [35]. It shows multiple characteristics of other nodes in the network, falling the efficiency of the fault-tolerant solutions.
5) *Flooding*: Given the complexity of the network and its impact on the longevity of our systems, the flooding and potential mitigation of the network is widespread. The current DDoS flood, the attack is the most worrying. The authors [10] conducted a completeanalysis of the algorithms and defensemethods. The main reason for this attack is the high traffic on the channel, which fills too many wasted messages.Essentially, one malicious node sends an ineffectual message and the attacker resends it to generate high traffic.

4.2 Man-in-the-Middle attacks

A "Man-in-the-Middle" attack allows an intruder to access the message transmitted among the nodes and is able to be utilized for thebenefits. Data encryption must be applied to eliminate the threat of this attack. The subsequent three attacks related to this kind of class are:

1) *Eavesdropping*: Eavesdropping is the process by which an attacker can access the communication channels. This is a negative attack except the assailant changes the packet accepted and transmits it to the contributors. This technique, known as the "playback attack", it is anextremelygeneralspoofing practice.
2) *Routing attack*: Because the routing messageis usually unencrypted, an attacker can transform the routing messageto create a routing loop that can considerably degrade the eminence of service.
3) *Replay attack*: Even if an attacker cannot get a signed packet and decrypt it, it can achieve the confidence of the router entity by resending the packet afterward. These attacks able to be overcome by means of message seriesstatistics and message verification codes. Sensor-based system routing algorithms [3] sometimes require notification. In this category of DoS attack, the malicious node transmits the wrong information to the adjacent nodes directed by the assist of these notifications [11].

Such attackswereable to be reduced with appropriate network protectionprocess. The securityschemesconsistofdynamic firewalls that smooth traffic flow, warning and control traffic with authentication in a two-way link authentication.

In the IoT, there is another problem when integrating difficultinheritanceschemes into the IoT infrastructure. In this case, an agent will be provided to transform the old interface and present security. However, in engineering systems, security is too highly valued. In [12], I talked about the protection and safety analysis of this businesscomputerization system. The IoT, guided by its success in the field of information technology, has led it to automation and industrial systems. While technology has become reliable for use in IT applications, the heterogeneity of available knowledge and the consequent limitation ofconsistent methods for specific utilize cases raises many unresolved issues.

V. SIGNIFICANCE OF SECURITY ROUTING IN IoT

With a proper routing strategy, a low-power wireless network environment is anextremely difficult task, mainly because of the inbuilt characteristics of everyfunction and the limitations of the sensors used. Therefore, the “Routing Protocol for Low Power and LossyNetworks (RPL)”[37] assumes that the route hastosettle into the constraints of a specific application area, and for everyrelevance area, the suitable RFC records the target task. Set optimization requirements in the target scenario.

The present RPL measurement[37] determines the significance of support methods for securing routing information'sswapamong sensors, so RPL determines the secure editions of diverse routing manageinformationin addition to three basic securityapproach in support of the following,

- *Integrity and Data Authenticity:*Thepresent RPL measurement [37] describes digital signatures that integrate MAC support and RSA with "SHA-256" using "128-bit AES" to support data integrity and reliability.
- *Semantic Security and Protection for Replay Attacks:*The"Control Consistency Check (CC)" control messages allow the discovery node to raise a response to confront to verify the existing counter value for another node. In thesecircumstances, the recipient starts the reorganizationbydistributing CC information to the source.

- *Key Management:*This indicates the encryption key required to handle the security of this message implicitly or explicitly. The "RFC 6550" [37] at presentdescribedissimilarideals for this area, therefore supporting diverse key management policies, specifically "group key", "key for each sensor pair" and "digital signature".

VI. LIMITATIONS AND OPEN ISSUES OF IoT SECURITY

After exploring various AD models, their limitations are summarized as follows and Table-1 presents the comparison of existing routing protocols advantages and disadvantage:

- Currently, most WSN applications are designed to process multi-variate data, but some models currently process uni-variate data. In multivariate data, the characteristicscollectively form an exception and the features may not be displayed alone. Some models handle multiple data but do not consider reducing data dimensions.
- Although the currently proposed models are planned to work online, the price of calculating their identification method is a foremost constraint leading to increased powerutilization.
- Currently, most existing models use a distributed structure from the commencement. However, these models have several disadvantages associated with the volume of the signifying model that needs to be connected among the nodes.In addition, generallypast distributed models unable to explain how to integrate local standard forms into global standard models. Finally, these templates did not specify appropriate thresholds for updating normal generic templates due to dynamic data changes.
- The ability to adapt to dynamic data changes built into some modern discovery models incurs furthercalculation costs that influence the appropriateness of real-time recognition and updates.
- Many of the proposed AD models overlook particular characteristics of WSN data that are "spatially" and "temporally" correlated. This characteristic is useful for progressing recognition precision. Also, theproperty/function associations that indicate reliance between functions are overlooked by generally existing tasks. Leveraging these functional correlations through functional reduction helps to maintain sensor energy.
- Some revised models, especially those based on statistics and taxonomy, have problems with parameter selection. Before testing, you need to set some parameters for the test model. The performance of various classification techniques, as SVM [17] can vary considerably due to transforms to certain clientconstraints. In an actual WSN application, it is not simple to specify the appropriate constraint values for every application. In addition, if the goal is to consider dynamic changes in WSN data, it is not appropriate to use fixed values.

Table-1: Comparison of Existing routing protocols and its Limitation

Year	Protocol	Advantages	Disadvantages
2014	DACR [39]	DACR has both delayed and certain data delivery with reliability in WSN, and with extends network lifetime.	In the case of navigation, DACR performance is not good, and productivity analysis in large scenarios does not reach the mark.
2016	QARP [40]	The suggestion protocol is useful for delay-sensitive applications.	It is not good for random deployment of sensor nodes.
2015	QoSR[41]	It selects the best route based on the power level to transmit using the "Bellman ford algorithm".	Controlling the overhead ratio is more in choosing a route.
2012	QoS-PSO [42]	The QoS-PSO algorithm is scalable and performs well in terms of reduced delay and good packet delivery rate in large networks.	Because of the overall energy cost, they are likely to be more than other protocols. The overhead of controlling path detection is greater.
2015	RPRA [43]	It is more suitable for large size network because it avoids congestion by providing more tracks for transmission.	It does not consider metric energy consumption to evolve.
2016	ProHet [44]	The main advantage of PropHet is to send an acknowledgment to the sender for its successful transfer.	The path selection stage is so complex that the level of energy consumption is high.
2016	PDORP [45]	It can be applied to many applications that require reliability and energy efficiency such as underwater monitoring.	It is not driven to dynamic environments.
2006	WASN [46]	The type of traffic priority is a feature of the proposed protocol. So the use of channels is good.	Low priority traffics are not well managed.
2015	MWTP [47]	Good performance for WANs and even shows lower power consumption.	In case of the network is large, bottlenecks may occur and shows low throughput.
2015	ACOFTR [48]	It is very useful for secure data transfer and fault tolerance is a key feature of the protocol.	It requires the most reliable technology to ensure safety. The energy level is not suitable.
2015	RESP [49]	Security is a fundamental function of the protocol because it encodes the transmitted data using Reed-Solomon encoding.	In order to encode the data before transmission, some smart technology is needed.
2014	P2PGDR [50]	The routing scheme is good for hybrid networks. The proposed agreement is characterized by market-based policies to support cooperative incentives.	As the flow ratio increases, the likelihood of delay is greater.
2015	HHR [51]	This is immense for mobile environments and can be applied to large networks. Deployment is usually fast.	Energy consumption and route maintenance are major issues in this protocol.
2014	PCDST [50]	It increases the throughput of network communication. An increase in the number of nodes in the network results in a reduction in power consumption.	PCDST does not consider QoS parameters such as delay, energy, reliability, and overhead. It does not apply to small networks.
2015	SPMR [51]	In a robust network design, performance is very good. This is also good for real-time traffic.	It is based on a tree-formed routing structure, so bottlenecks can occur.
2014	TRRP [52]	It provides a robust routing construct and is therefore ideal for	In the construction of routing paths, the energy consumption

6.1 Open Issues in IoT Security

- *Online detection:* It is recommended to bring the detection process online to assemble the needs of a few"real-time" WSN applications. Many existing models have been declared suitable for online testing, but the detection methods employed result in high energy consumption. Therefore, a lighter detection method is required.
- *Adaptive Detection*: Since sensor data has dynamic flow properties, it is necessary to update the detection model to minimize false detection and improve detection accuracy. Several recommended adaptive strategies have high calculationcomplication, which influences their applicability to online recognition. As a result, it is necessary to modify thisscheme or propose novel lightweight strategies.
- *Feature/Attribute correlations*: The "temporal" and "spatial" correlation of sensor data have to be utilized to simultaneously progress the usefulness and competence of the test. These links have to be used in conjunction with feature links to increase usefulness and effectiveness.
- *Parameter tuning*: To decreaseindividualinvolvementanddoes not set any parameters manually when designing an AD model. To reduce human intervention, it is recommended to use the automatic parameter tuning method.

In [28], [29] the authors proposed the transfer of cryptographic computations to a key exchange on a resource-rich proxy in a collaboration scheme. However, these two systems increase communication costs, the time needed to set up a secret key, and are vulnerable to DoSattacks. The "Slimfit" [38] moderate communication costs throughestablishing a compression layer in the protocol layer.

The "HIP-PSK" is proposed for authentication by O. Garcia-Morchon et al. [32],but, in common, PSK-supported systems do not offerhigh-quality security. Even the "Lightweight HIP (LHIP)" [28] also does not executeseveral security methods for the verification and encryption, therefore is not suitable for IoT-based systems.

T. Kothmayr et al. [27] proposed a DTLS scheme based on the "X.509 certificate" for reciprocatedverification of restricted appliances. S. Gusmeroli et al. [36] describe two-factor verificationmethod was designed that allows communication peers to use mutual authentication for implicit authentication. However, neither of the proposed proposals considers the solution but checks the revocation list that requires the IoTappliance to development the certificate sequence.

The "6LoWPAN" header firmnesspractice is used to decrease the dimension of the "DTLS" header is discussed by S. Raza et al. [16]. The proposed method eliminates the packet divisions. This decreases "packet loss", "packet processing time", "retransmission rate" and "energy consumption". However, the workdescriptionnot able tomaintain compatibility with the criterion"DTLS" protocol, especially in terms of header compression.

Distributed methods, alternatively, are well suited for these real-time IoTstructures and relevance, because appliances can executeprocedure tasks and determine permissions. Decentralized methods are highly scalable, but they are complex to manage and therefore lack interoperability. Distributed methods perform poorly in terms of memory efficiency due to the fact that guidelines, undisclosed contexts, and assessment algorithms are accumulated in appliance storage.

VII. CONCLUSION

The survey paper provides insights into the security issues and challenges of routing IoT in wireless communications. First, it discusses the security issues and challenges of WSNs associated with today's wireless communication scenarios. Second, it discusses various security methods and anomaly prediction methods associated with WSN. Third, it introduces the security of the IoT and its significance analysis in the secure routing of the IoT. Finally, it highlights the limitations and openness of IoT security and provides a potential research direction for IoT routing. To the best of our knowledge, this survey is the first of its kind to provide researchers and readers with a broad overview of the different research results and suggested solutions for secure routing issues between IoT devices.

REFERENCES

1. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communication Survey Tutorial, Vol. 17, pp. 2347–2376, 2015.
2. CISCO, The Internet of Everything(IoE): Connections Counter (December 2, 2014). Available: http://newsroom.cisco.com/feature-content?type.webcontent&articleId.1208342
3. M. Asif, S. Khan, R. Ahmad, M. Sohail, D. Singh, "Quality of Service of Routing Protocols in Wireless Sensor Networks: A Review", IEEE Access, Vol. 5, pp. 1846 - 1871, 2017.
4. Y. Tahir, S. Yang, J. McCann, "BRPL: Backpressure RPL for High-Throughput and Mobile IoTs", IEEE Transactions on Mobile Computing, Vol. 17(1), pp. 29 - 43, 2018.
5. Wang, K. Viswanathan, L. Choudur, V. Talwar, W. Satterfield, K. Schwan, "Statistical techniques for online anomaly detection in data centers", IEEE Integrated Network Management, pp. 385–392, 2011.
6. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez, "Anomaly-based network intrusion detection: techniques, systems, and challenges", Computer Security, Vol. 28(1-2), pp. 18–28, 2009.
7. A. P. Abidoye, I. C. Obagbuwa, "Models for integrating wireless sensor networks into the Internet of Things", IET Wireless Sensor Systems, Vol. 7(3), pp. 65 - 72, 2017.
8. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.
9. M. Frustaci, P. Pace, G. Aloi, G. Fortino, "Evaluating critical security issues of the IoT world: Present and Future challenges", IEEE Internet of Things Journal, Vol. 5(4), pp. 1 - 1, 2018.
10. M. Guri, Y. Mirsky, Y. Elovici, "9-1-1 DDoS: Attacks, Analysis and Mitigation", IEEE European Symposium on Security and Privacy (EuroS&P), pp. 218 - 232, 2017.
11. Cervantes, D. Poplade, M. Nogueira, A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for the Internet of Things", IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606 - 611, 2015.
12. S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia, G. Bianchi, "OAuth-IoT: An access control framework for the Internet of Things based on open standards", IEEE Symposium on Computers and Communications (ISCC), pp. 676 - 681, 2017.

13. S. Vashi, J. Ram, J. Modi, S. Verma, C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues", International Conference on I-SMAC, pp. 492 - 496, 2017.
14. P. Varga, S. Plosz, G. Soos, C. Hegedus, "Security threats and issues in automation IoT", IEEE 13th International Workshop on Factory Communication Systems (WFCS), pp. 1 - 6, 2017.
15. S. Verma, Y. Kawamoto, Z. Md. Fadlullah, H. Nishiyama, N. Kato, "A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues", IEEE Communications Surveys & Tutorials, Vol. 19(3), pp. 1457 - 1477, 2017.
16. S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure coap for the IoT", Sensors Journal, IEEE, 2013.
17. A. Bhargava, A. S. Raghuvanshi, "Anomaly Detection in Wireless Sensor Networks Using S-Transform in Combination with SVM", 5th International Conference on Computational Intelligence and Communication Networks (CICN), pp. 111-116, 2013.
18. S. Che, R.Feng, X. Liang, X. Wang, "A lightweight trust management based on Bayesian and Entropy for wireless sensor networks", Secure Communication Network, Vol. 8, pp. 168–75, 2015.
19. H. Suo, J. Wan, C. Zou, J. Liu, "Security in the Internet of Things: A Review", IEEE International Conference on Computer Science and Electronics Engineering, pp. 648-651, 2012.
20. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", IEEE Internet of Things Journal, Vol. 4(5), pp. 1125 - 1142, 2017.
21. M. Hossain, R. Hasan, A. Skjellum, "Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems", IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 220 - 225, 2017.
22. Zucchetto, A. Zanella, "Uncoordinated Access Schemes for the IoT: Approaches, Regulations, and Performance", IEEE Communications Magazine, Vol. 55(9), pp. 48 - 54, 2017.
23. H. Ning, H. Liu, L. T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", IEEE Transactions on Parallel and Distributed Systems, Vol. 26(3), pp. 657 - 667, 2015.
24. Z. Ren, X. Liu, R. Ye, T. Zhang, "Security and privacy on the internet of things", 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), pp. 140 - 144, 2017.
25. R. H. Weber, "Internet of Things—New Security and Privacy Challenges", Computer Law and Security Review, Vol. 26, pp. 23-30, 2010.
26. Airehrour, J. Gutierrez, S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism", 26th International Telecommunication Networks and Applications Conference (ITNAC), pp. 115 - 120, 2016.
27. T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication", 37th IEEE Conference on Local Computer Networks - Workshops, 2012.
28. Y. B. Saied, A. Olivereau, "D-HIP: A distributed key exchange scheme for HIP-based Internet of Things", IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2012.
29. Y. Ben Saied, A. Olivereau, "TEX: A distributed key exchange scheme for HIP-based Internet of Things", IEEE International Conference on Communications and Networking, 2012.
30. J. Granjal, E. Monteiro, J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communications Surveys & Tutorials, Vol. 17(3), pp. 1294 - 1312, 2015.
31. M. Díaz, C. Martín, B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing", Journal of Networking and Computer App, Vol. 67, pp. 99–117, 2016.
32. O. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and R. Hummen, "Security Considerations in the IP-based IoT", RFC, 2013.
33. A. E. Hajjar, G. Roussos, M. Paterson, "Secure routing in IoT networks with SISLOF", Global Internet of Things Summit (GIoTS), pp. 1 - 6, 2017.
34. D. Shin, V. Sharma, J. Kim, S. Kwon, I. You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks", IEEE Access, Vol. 5, pp. 11100 - 11117, 2017.
35. K. Zhang, X. Liang, R. Lu, X. Shen, "Sybil Attacks and Their Defenses in the Internet of Things", IEEE Internet of Things Journal,Vol. 1(5), pp. 372 - 383, 2014.
36. S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things", Mathematical and Computer Modelling, 2013.
37. R. Alexander, A. Brandt, J. Vasseur, et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks; RFC 6550", IETF Secretariat: Fremont, CA, USA, 2012.
38. R. Hummen, J. Hiller, M. Henze, and K. Wehrle, "Slimfit: A HIP DEX compression layer for the IP-based IoT", IEEE International Conference on Communications and Networking, 2013.
39. M. A. Razzaque, M. H. U. Ahmed, C. S. Hong, and S. Lee, "QoS-aware distributed adaptive cooperative routing in wireless sensor networks", Ad Hoc Network, vol. 19, pp. 28-42, Aug. 2014.
40. B. Bhuyan and N. Sarma, "AQoS aware routing protocol in wireless sensor networks with mobile base stations", in Proc. Int. Conf. Internet Things Cloud Computing, pp. 1-5, 2016.
41. J. Levendovszky and H. N. Thai, "Quality-of-service routing protocol for wireless sensor networks", Journal Information Technology Software Engineering, vol. 4, no. 2, p. 133, 2015.
42. M. Liu, S. Xu, and S. Sun, "An agent-assisted QoS-based routing algorithm for wireless sensor networks", Journal Network Computing Appl., vol. 35, no. 1, pp. 29-36, 2012.
43. M. Tang, X. Lin, and M. Palesi, "Routing pressure: A channel-related and traffic-aware metric of routing algorithm", IEEE Trans. Parallel Distributed Syst., vol. 26, no. 3, pp. 891-901, Mar. 2015.
44. X. Chen et al., "ProHet: A probabilistic routing protocol with an assured delivery rate in wireless heterogeneous sensor networks", IEEE Trans. Wireless Comm., vol. 12, no. 4, pp. 1524-1531, 2013.
45. G. S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song, and S. H. Ahmed, "Energy-efficient direction-based PDORP routing protocol for WSN", IEEE Access, vol. 4, pp. 3182-3194, 2016.
46. A. Boukerche, R. B. Araujo, and L. Villas, "A wireless actor and sensor networks QoS-aware routing protocol for the emergency preparedness class of applications", in Proc. 31st IEEE Conf. Local Comput. Network, Tampa, FL, USA, pp. 832-839, 2006.
47. S. Gupta and R. Bose, "Energy-efficient joint routing and power allocation optimization in bit error rate constrained multihop wireless networks", IET Commun., vol. 9, no. 9, pp. 1174-1181, Jun. 2015.
48. S. Surendran and S. Prakash, "An ACO look-ahead approach to QOS enabled fault-tolerant routing in MANETs", China Commun., vol. 12, no. 8, pp. 93-110, 2015.
49. H. Shen, Z. Li, and L. Yu, "A P2P-based market-guided distributed routing mechanism for high-throughput hybrid wireless networks", IEEE Trans. Mobile Comput., vol. 14, no. 2, pp. 245-260, Feb. 2015.
50. J. R. Diaz, J. Lloret, J. M. Jimenez, and J. J. P. C. Rodrigues, "A QoS-based wireless multimedia sensor cluster protocol", International Journal Distrib. Sensor Network, 2014.
51. D. Jie, W. Xiong, W. Sheng, and X. Shizhong, "HHR: Hierarchical hybrid routing scheme for information-centric network", China Commun., vol. 12, no . 6, pp. 141-153, 2015.
52. J. Peng, J. Jingqi, S. Qiushuo, and Z. Songyang, "A noble cross-layer protocol for QoS optimization in wireless sensor networks", in Proc. 26th Chin. Control Decision Conf. (CCDC), pp. 2430-2434, 2014.
53. A. Fréchette, F. B. Shepherd, M. K. Thottan, and P. J. Winzer, "Shortest path versus multi-hub routing in networks with uncertain demand", IEEE/ACM Trans. Network, vol. 23, no. 6, pp. 1931-1943, Dec. 2015.
54. Y. Gao, W. Dong, C. Chen, J. Bu, and X. Liu, "Towards reconstructing routing paths in large scale sensor networks", IEEE Trans. Comput., vol. 65, no. 1, pp. 281-293, Jan. 2016.
55. T. Meng, F. Wu, Z. Yang, G. Chen, and A. V. Vasilakos, "Spatial reusability-aware routing in multi-hop wireless networks", IEEE Trans. Comput., vol. 65, no. 1, pp. 244-255, Jan. 2016.

AUTHORS PROFILE

Saibabugutta, currently pursuing his ph.D degree in Electronics and Communication Engineering from Bhagwantuniversity in the field of Security Issues and Challenges in IoT Routing over Wireless Communication. he obtained his Master 's degree in the field of Electronics and Communication Engineering in 2013 from JNTUH. He obtained his Bachelor 's degree in the field of Electronics and Communication Engineering in 2010.

Anuj Jain, is working as a Professor in Lovely Professional University, Punjab India. He obtained his Bachelor's degree in the field of Instrumentation in 2002 & Master's degree in 2005 with distinction in Electronics and Communication Engineering. After completing his Masters studies, he is working in teaching field. He Completed his Ph.D. in the field of Electronics and Communication at Mewar University, Chittorgarh, Rajasthan in 2016. During his study and teaching Profession he published 21 research papers in different referred journals and Conferences.10 PG(MTech) and 1 PhD completed under his guidance till now.

V. K. Sharma(1961) received his bachelordegree from KREC Surathkal in 1984, M.Tech. in Power Electronics from IIT Delhiin 1993, and PhD from IIT Delhi in 2000.He is recipient of various scholarships,Railway Board Medal and has completed afew AICTE sponsored projects. He hasworked with College of Engineering, at Pravaranagar, and JamiaMilliaIslamia University in NewDelhi. Currently, he is a full Professor in the Department ofElectronics & Telecommunication Engineering at MaharashtraAcademy of Engineering, Alandi, under Pune University,India. He has visited USA, Germany Malayasia, and HongKong to present his research findings in IEEE conferences. Hehas worked as post doc fellow during 2001-2002 at Ecoledetechnologiessuperieure, Montreal, Canada. He is a regularreviewer for several IEEE conferences and national/international journals. He is a member of Institutionof Engineers (India) and Fellow of IETE, India. His researchinterests include power electronics, and application ofcomputer communication in hybrid electric vehicle