Internet of Things: Attacks and Defences

Richa Sarma
Indian Institute of Information Technology
Guwahati, Assam, India
Email: richa@iiitg.ac.in

Ferdous Ahmed Barbhuiya
Indian Institute of Information Technology
Guwahati, Assam, India
Email: ferdous@iiitg.ac.in

***Abstract*—Ever since the introduction of IoT, it has gained much popularity and is being widely used nowadays. However, assimilation of these everyday objects also introduced many security threats, which have become a matter of concern among the research fraternity. Unfortunately, the security threats and their corresponding countermeasures are not well organized in the context of IoT. Therefore, through this survey, we attempt to provide a list of attacks in each layer of IoT, suggested countermeasures in literature and possible research direction in the area.**

***Index Terms*—IoT, Security Challenges, Countermeasures, Attacks**

I. Introduction

With the advancement of technology, a new class of devices/objects like mobiles, PDAs, various sensors, actuators etc. have emerged, which also brought the idea for interconnecting these devices through various technologies. This has lead to the development of a new technology called "Internet of things" (IoT). It enables objects used in daily life to communicate with each other without regular human intervention. Through this technology, various heterogeneous objects (provided with unique identifiers) can be interconnected and exchange data over the Internet. The objects may include living things, sensor or anything that can react autonomously to any change in the environment. Users of IoT are increasing exponentially and it is expected that by 2020, there will be 50 billion connected devices [1].

IoT is a fusion of heterogeneous devices, so all the threats and possible attacks that lie within these devices may propagate to IoT as well, which has made the security of IoT more complex. With the fast adoption of IoT, there is increased urgency of addressing these security threats. Several surveys have been conducted on the security of IoT. Bakshi *et al.* [2] analyzed the CISCO's and Microsoft Azure architecture of IoT. Moreover brief discussion of security threats on IoT had also been done. Yang *et al.* [3] discussed limitations of IoT devices in terms of battery life and computational power, and provided solutions in order to overcome these limitations. The paper reviewed existing authentication schemes and architecture and discussed the proposed security measures in layer-wise fashion. Oracevic *et al.* [4] analyzed different proposed schemes and classified them on the basis of the security requirements achieved by them. Lin *et al.* [5] focused on the integration of IoT with fog/edge computing and presented various issues related to it. The paper also discussed various existing architectures of IoT, including the three-layered architecture and SOA based four-layered architecture, enabling technologies and challenges in different layers. Nia *et al.* [6] discussed the CISCO's seven-layered architecture of IoT. The paper analyzed the possible attacks and suggested countermeasures at the edge layer (edge nodes, communication, and edge computing), but they only provided the mapping of countermeasures of the discussed attacks without any proper explanation. Based on different directions in which an IoT device can be attacked, Andrea *et al.* [7] classified attacks in a unique way i.e. physical attacks, network attacks, software attacks, as well as attacks on encryption schemes and discussed layer-specific countermeasures.

II. Motivation and Contributions

Why to study security issues in IoT ? Though several security issues and respective solutions of the traditional network have been studied in literature, the issues and security solutions of IoT is different from traditional network in several ways. Some of them are:

- IoT composed of miniature objects like RFID, WSN which have low computational power and storage capacity. The communicating objects in traditional network involves Computer, Laptop, etc. which are rich in resources. So, most of the algorithms, protocols suitable for traditional network devices do not suit IoT devices.
- Though the communicating devices of traditional network are different, they have operating system (usually Windows/UNIX) which have almost similar data formats. However, IoT devices, programs are embedded in the chip. Different hardware have different data format which leads to heterogeneous data.
- IoT consists of several devices which exchange data and perform various functions of our day to day life. In other ways these devices keep track of our life. It will be a matter of concern if these devices start operating on the instruction of adversary or leak information about our daily life. But the same is not with traditional network, if we do not give any input then hardly any information about our everyday life will be tracked.

A. Problems in current works

In the current scenario, several efforts [2]- [7] have been made to discover possible attacks and provide countermeasures against them. Though various surveys have been conducted focusing the security of IoT, they fail to discuss encountered attacks and defensive measures addressed against each attacks in a well-structured way. Hence, this paper presents an extensive survey on various attacks encountered in each layer of IoT along with the mitigation techniques for each of the attacks suggested against them . Also, it aims at making the reader well aware of the encountered attacks, how they have been addressed and reflects on open and not fully addressed issues, so that a further study can be done on the subject.

B. Contributions

Contributions of this work can be summarized as follows:

- Basic architecture of IoT is discussed.
- Layerwise classification of security threats in IoT.
- Brief description of these security threats.
- Various countermeasures suggested for each type of security threat.
- Challenges and Research directions.

978-1-7281-1557-3/19/$31.00 ©2019 IEEE

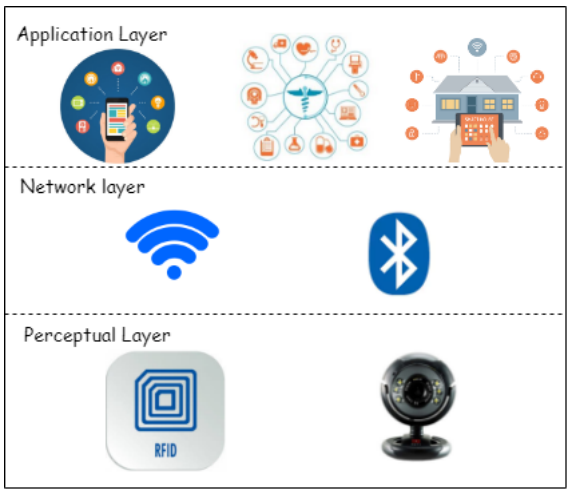

Fig. 1: Three-layered Architecture of IoT

III. Overview of IoT and its Security Requirements

A. Enabling Technologies

Deployment of IoT became possible through some network technologies such as:

- *Radio Frequency Identification (RFID)*: It is a type of wireless technology that uses electromagnetic waves to uniquely identify and track objects. An RFID system consists of three basic components: *RFID tags*, *RFID reader* and *antenna*.
- *Wireless Sensor Networks (WSN)*: It is an interconnection of several small sized, low cost and low power autonomous devices. These devices consist of sensors which have the capability to monitor, collect and transmit the information gathered from the environment.
- *Cloud Computing*: As smart devices are constrained by various resources, the data collected by them are outsourced to cloud for storage and intelligent processing.

B. Security Requirements

An IoT system must have the following security requirements as described in [6]:

- *Confidentiality*: It should ensure that only the intended users should be able to access the data.
- *Integrity*: It should not allow unauthorized modifications.
- *Availability*: The authorized users must be able to access the information when required.
- *Auditability*: It must perform time to time recording of the actions.
- *Privacy*: It must follow privacy policies and enable the corresponding user to control their personal data.
- *Accountability*: The users of the system must be answerable for their actions.
- *Non-repudiation*: The users of the system should not be able to deny the actions performed by them.

C. IoT Architecture

According to Jia *et al.* [8], IoT can be represented as a three-layered architecture as shown in Figure 1, which are described as follows:

1) *Perception layer*: The main objective of this layer is to sense, collect information or identify other smart objects in the environment. Information collected includes the physical parameters such as location, temperature, humidity, vibration etc., depending upon the type of devices used (like GPS, temperature sensor etc.).
2) *Network Layer*: This layer is mainly responsible for interconnection of different IoT devices present in the network. It is achieved by using some of the technologies such as Bluetooth, Wifi etc.
3) *Application Layer*: The application layer is also known as "Service Layer". The layer helps in the processing of data and provide services requested by the end-users.

IV. Classification of IoT attacks and Countermeasures

In this section, various attacks encountered in different layers of IoT as well as Multi-layer attacks which affect more than one layer is discussed and suggested countermeasures are provided. The summary of layer-wise classification of attacks and its effects are shown in Table I.

Layer	Attack	Against
Perception Layer	Node Capture	All
	Replay Attacks	C, I, AC
	Eavesdropping	C, NR, P
	Interference	A, I
	Sleep Deprivation	A
	Physical Damage	All
Network Layer	Sinkhole	C, I, AC, NR, P
	RFID cloning and Spoofing	All
	Sybil attack	NR, C, P, I, AC
	Worm hole	I, C, AC, P, NR
	Hello flood	AC, I, C, NR, P
	Selective forwarding	C, AC, I, NR, P
Application Layer	Malicious code injection	All
	Phishing attack	P
	Buffer overflow attack	A
Multi-Layer	Denial of Service(DoS)	All
	Side channel analysis	C, AU, NR, P
	Man-in-the-middle attack(MITM)	C, I, AC, NR, P

TABLE I: Summary of attacks and their effects
Abbreviations: C= Confidentiality, I= Integrity, A= Availability, AU= Auditability, P= Privacy, AC= Accountability, NR= Non-repudiation

A. Perception Layer attacks

1) *Node Capture*: In this type of attack, the adversary controls the node either by making some modifications or physically replacing it. A type of node capture attack is *node replication attack* [9] in which the attacker creates a replica of an existing node and adds the replica to the set of existing nodes to the network.
Countermeasure: Node capture attack can be mitigated by strengthening the Cryptographic schemes [6]. The random-pairwise keys scheme [10] is a cryptographic scheme which uses a node-to-node authentication strategy to counter this attack. Another solution is use of Tamper resistant nodes [11] but it incurs a high cost.
2) *Replay Attacks*: Usually Replay attack [12] is launched during the authentication phase. In this type of attack, the attacker sends some data which has been already received by the destination host from the victim in order to obtain the trust and thereby enter the system.
Countermeasure: In recent years, a certain number of user authentication schemes has been proposed for IoT, which mostly uses timestamp mechanism [13] or nonce [14]. The challenge-response mechanism [15], is also suggested for countering this attack.
3) *Eavesdropping*: In this type of attack [16], the attacker secretly listens to private communication of two parties

without their knowledge. The aim is to obtain some confidential data or collect information.
Countermeasure: To mitigate eavesdropping, encryption algorithms must be strengthened [5]. Though there are many other encryption algorithms like AES, RSA, El-Gamal etc. but ECC is widely suggested because of the resource constraint nature of IoT devices [17].

JAMMING

4) *Interference*: In this attack [18], the attacker sends some noise signals to interfere with the signals . It leads to collisions or loss of packet which makes the sender resend the packets requiring more time and energy.
Countermeasure: For mitigating interference, a number of antenna array techniques have been studied [11] in the literature. Spread spectrum communication, in which the signals are distributed over a range of frequencies, is also suggested as a defensive measure. Other solutions commonly used for identifying this attack include Receive Signal Strength Index (RSSI) values [19] or Packets Delivery Ratio (PDR) [20].
5) *Sleep Deprivation Attacks*: Most of the IoT devices are of low power, so to reduce the power consumption and extend their life, the devices are put in sleep mode time to time. The sleep deprivation attack [6] makes the IoT devices awake all the time until they have a power failure and stop functioning.
Countermeasure: In [21], an energy harvest scheme *Pro-Energy* has been proposed, which created the provision of harvesting energy from the external environment (solar, wind traces etc.). Moreover, other mechanisms like the random vote scheme, the round robin scheme, and the hash-based scheme have also been found as means to mitigate this attack [22]. Use of secured dutycycle mechanism [5] has also been suggested.
6) *Physical Damage:* Physical attack [7] can turn out to be the easiest of all attacks if the place is not secured where the devices are hosted. It includes stealing or breaking the device so as to make it unavailable for service.
Countermeasure: Since the attacker has to be present physically to attack the system, to mitigate physical attack [7], devices should be kept in a protected area.

B. Network Layer attacks

intressante

1) *RFID Cloning and Spoofing*: All RFID tags have unique identities which distinguish them. If the RFID tag does not employ any security features or the security features are not that strong enough then cloning involves replicating the tags ID and any data related to the clone tag [6]. Another attack, similar to cloning is spoofing [5] where the attacker emulates the original tag and gain privileges. An attacker may use RFID cloning or spoofing to get secret information like ATM pin, password etc.
Countermeasure: To mitigate these attacks strong authentication mechanism is required. Physical Unclonable Function (PUF) [23], an authentication mechanism that uses a one-way function and challenge-response mechanism is widely used to mitigate RFID tag cloning. Several other authentication protocols based on cryptographic primitives like bitwise operator(XOR), pseudo-random numbers or hash-functions has also been proposed against such attacks.
2) *Sinkhole Attack*: Sinkhole attack [5], also known as *"black hole attack"*, is a type of attack in which compromised node tries to attract network traffic towards itself using false routing information. The compromised node could then perform selective forwarding or data manipulation.
Countermeasure: Several authors have discussed Sinkhole attacks [24], [25] in literature. In [24] a trust-based scheme is proposed for the routing protocol to detect and mitigate sinkhole attacks. Similarly, in [25] a Statistical En-route Filtering mechanism is proposed for detecting and dropping false reports provided by the attacker.
3) *Sybil Attack*: In this type of attack [26], a malicious node claims the identity of many other nodes in the network. The goal of the attacker is to spread spam, violate users privacy or manipulate reputation system.
Countermeasure: Mutual authentication of the nodes in contact can be used to mitigate this attack. In [27], authors have used game theory approach to detect Sybil nodes. Reputation technique [28] has also been suggested as a defensive measure.
4) *Worm hole Attack*: The Wormhole attack [29] can be launched without compromising any node, and even if authenticity and confidentiality infrastructure is provided. The malicious node captures some packets from one location in the network and forwards the same or selectively to the other distant location in the network.
Countermeasure: Most of the detection or mitigation techniques use distance or time analysis [30], [31]. Perrig *et al.* [30] proposes a packet leashes mechanism to detect and defend against wormhole attacks. Authors in [31] uses Spanning Trees as a defensive measure.

FLOODINGATACK

5) *Hello Flood*: To launch Hello Flood attack [6], a malicious node from a distant point uses high transmission power and sends hello messages to assure the nodes that it is their neighbor. The adversary may broadcast a fake high-quality route which is far away from making all the packets to route multi-hop. This increases the delay and decreases network performance.
Countermeasure: As the attacker uses hello message as a weapon, verifying the bi-directionality of the link prior to taking any action over the message received from that link has been suggested [32]. However, in certain circumstances like if the transmitter is powerful or sensitive enough then the attacker can bypass it. In [32], execution of identity verification protocol between the neighboring nodes is suggested which is considered as an effective solution for mitigation of hello flood attacks.
6) *Selective forwarding*: In a multi-hop network, if one of the intermediate nodes turns out to be malicious then it may refuse to forward all the packets and forward only some of them to the next node resulting in selective forwarding [33] of the packet.
Countermeasure: Multi-path routing [34] can be used to mitigate this attack. Moreover, braided paths [35], which may have common nodes but no any common links,is also used as a defensive measure.

C. Application Layer attacks

NODE CAPTURE

1) *Malicious code injection*: The adversary can inject malicious code in the node and control the IoT devices. The malicious code may crash the system, steal or tamper the confidentiality of the data [5].
Countermeasure: Code authentication schemes are designed to protect devices from malicious code injection attack. Secure booting [36], a feature introduced in OS

NODE CAPTURE

(Windows 8,10), prevents malicious software applications from loading during the system start-up process. In [13], generation of process-specific randomized instruction sets within the same system is also suggested.

2) *Phishing Attack*: This type of attack is launched with the aim of stealing user data like login details, credit card number etc. The attacker sends some mail or text message and somehow tricks the user to click the link attached to it, which reveals the secret information.
Countermeasure: Several anti-phishing techniques like certification by third party [37], password-based [38] or URL based [39] are suggested in literature. Moreover, authentication schemes which include user authentication [40] and email authentication [41] are also considered as effective solutions to counter phishing attack.
3) *Buffer Overflow Attack*: A buffer is a temporary storage which can store a fixed amount of data. The attacker launches the buffer overflow attack [18] by adding irrelevant data which overwrites the data held there and even may crash the system.
Countermeasure: Crispin Cowan *et al.* [42] designed a compiler named StackGuard, programs compiled using it are considered safe from buffer-flow attack. Similarly, Libsafe and Libverify [43], a library where the programs linked to any system need to be loaded beforehand to counter this attack.

D. Multi-layer attacks

1) *Denial of Service(DoS) Attacks*: DoS attacks [44] are of several forms like Interference, Selective dropping, malicious code injection etc. that are encountered in different layers. Other attacks like excessive consumption of resources like bandwidth, memory or processor time also come under DoS attack. The aim of this attack is to make the service unavailable for access or useless.
Countermeasure: As DoS attacks are of various forms, the type of countermeasure depends upon the type of misbehavior. Techniques mostly used to counter them are end-to-end authentication [45], filtering [46] etc.
2) *Side Channel Analysis Attack:* In this attack [47], the attacker aims to extract the secret data by applying some techniques outside the normal computation. The side-channel analysis includes analysis of computation time, power consumption, electromagnetic emission etc.
Countermeasure: For mitigation of Side channel attacks, there is a need of secure encryption algorithm as the existing and the most secure ones (AES, RSA etc.) suffer from side channel attack [47]. Some LEA (Lightweight Encryption Algorithm) specially designed for IoT devices are also suggested in [48]. Moreover, for protecting crypto-systems against timing attacks randomization technique [49] is also suggested.
3) *Man-in-the middle(MITM) attack*: In this attack [5], the attacker inserts a malicious device into a conversation between two parties, impersonates both parties and gains access to information transmitted between them.
Countermeasure: As MITM attacks occur in different layers of IoT, mitigation techniques depends on the type of MITM attack. The attack can be countered by the using efficient cryptographic schemes. Public key cryptography are widely used to counter this attack [50]. Other solutions like Voting [51], use of additional hardware [52] are also considered effective countermeasures.

V. Challenges and Research directions

Security is a key aspect in determining the future of IoT. Various attacks have been detected and their corresponding countermeasures have also been suggested in the above sections. As IoT is still in its early stage, research to identify more potential threats is ongoing. It has been found that most of the solutions to overcome these attacks show inconsistency in presence of heterogeneous devices or lack some of the features that may give birth to another form of attack. Following are some of the research areas that need serious attention for the proper deployment of IoT:

- As IoT devices are resource constraint products, most of the effective network protocols for Key management, Network security etc. do not comply with IoT devices. Some of the lightweight protocols suggested have one or other drawbacks. Therefore, designing lightweight protocols suitable for IoT devices is a prerequisite.
- With the popularity of IoT, a number of applications have developed that support this technology. This has brought the problem of integrating the data generated by these heterogeneous devices which may have different representation models of their respective data. Hence, there is a need for a common data model that can be incorporated by all these heterogeneous devices.
- IoT is accepted widely and the applications joining the IoT ecosystem is growing exponentially. Therefore, scalability is one of the key factor which may be a hindrance for its proper development.
- In IoT devices, lack of proper authentication mechanism may lead to various attacks like Node Capture attack, Replay attack, Spoofing etc. Usually, to authenticate devices in the network, cryptographic means are used which themselves face potential threats and considered not suitable for IoT devices as they have high computation cost. Therefore, there is a need for an authentication scheme specifically designed for miniature IoT devices.
- IoT devices responsible for providing numerous services in our everyday life may leak information like health status, location, and lifestyle of the owner. Therefore, there is a need for time to time monitoring of the actions performed by these autonomous devices. Hence, auditing the overall IoT system is an important area of research.

VI. Conclusion

The emergence of IoT has brought a revolution in the world of technology. Like other network based technologies, IoT also suffers from security threats which hinder its development. In this survey, security threats that exist in different layers of IoT and suggested countermeasures have been provided. Furthermore, challenges and research directions have also been discussed that can contribute to the development of IoT .

References

[1] D. Evans, "The Internet of Things, How the Next Evolution of the Internet is changing everything," *Whitepaper, Cisco Internet Business Solutions Group*, vol. 1, pp. 1–12, 2011.
[2] Z. Bakhshi, A. Balador, and J. Mustafa, "Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models," in *IEEE WCNCW*, April 2018, pp. 173–178.
[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct 2017.
[4] A. Oracevic, S. Dilek, and S. Ozdemir, "Security in Internet of Things: A survey," in *ISNCC*, May 2017, pp. 1–6.

[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[6] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, Oct 2017.

[7] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *ISCC*, July 2015, pp. 180–187.

[8] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *CECNet*, April 2012, pp. 1282–1285.

[9] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *IEEE Symposium on Security and Privacy*, May 2005, pp. 49–63.

[10] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Symposium on Security and Privacy*, May 2003, pp. 197–213.

[11] L. Buttyán and J.-P. Hubaux, "Stimulating Cooperation in Self-organizing Mobile Ad Hoc Networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, Oct. 2003.

[12] Y. Mo and B. Sinopoli, "Secure control against replay attacks," *Allerton Conference on Communication, Control, and Computing*, pp. 911–918, 2009.

[13] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[14] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for iot devices using RFID tags," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1085–1102, Mar 2017.

[15] Y. Feng, W. Wang, Y. Weng, and H. Zhang, "A Replay-Attack Resistant Authentication Scheme for the Internet of Things," in *IEEE EUC*, vol. 1, July 2017, pp. 541–547.

[16] G. P. Hancke, "Eavesdropping Attacks on High-Frequency RFID Tokens," in *RFIDSec*, 2008.

[17] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," in *Sensors*, 2014.

[18] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Information Systems Frontiers*, vol. 12, no. 5, pp. 491–505, Nov 2010.

[19] J. H. Hauer, A. Willig, and A. Wolisz, "Mitigating the Effects of RF Interference through RSSI-Based Error Recovery," in *Wireless Sensor Networks*. Springer Berlin Heidelberg, 2010, pp. 224–239.

[20] G. Zhou, T. He, J. A. Stankovic, and T. Abdelzaher, "RID: radio interference detection in wireless sensor networks," in *IEEE Joint Conference of the IEEE Computer and Communications Societies.*, vol. 2, March 2005, pp. 891–901 vol. 2.

[21] A. Cammarano, C. Petrioli, and D. Spenza, "Pro-Energy: A novel energy prediction model for solar and wind energy-harvesting wireless sensor networks," in *IEEE MASS*, Oct 2012, pp. 75–83.

[22] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," *International Journal of Distributed Sensor Networks*, vol. 2, no. 3, pp. 267–287, 2006.

[23] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," in *IEEE RFID*, April 2008, pp. 58–64.

[24] A. A. Pirzada and C. McDonald, "Circumventing Sinkholes and Wormholes in Wireless Sensor Networks," in *IWWAN*, 2005.

[25] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in *IEEE INFOCOM*, vol. 4, March 2004, pp. 2446–2457 vol.4.

[26] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil Attacks and Their Defenses in the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, Oct 2014.

[27] Y. B. Reddy, "A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks," in *SENSORCOMM*, June 2009, pp. 462–468.

[28] J. Dinger and H. Hartenstein, "Defending the Sybil attack in P2P networks: taxonomy, challenges, and a proposal for self-registration," in *ARES*, April 2006, pp. 8 pp.–763.

[29] R. S. S. K. Garcia-Morchon, S. Kumar and R. Hummen, "Security considerations in the ip-based internet of things," 2013. [Online]. Available: https://tools.ietf.org/html/draft-garcia-core-security-06

[30] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *IEEE INFOCOM*, vol. 3, March 2003, pp. 1976–1986 vol.3.

[31] K. Harsnyi, A. Kiss, and T. Szirnyi, "Wormhole detection in wireless sensor networks using spanning trees," in *IEEE Future IoT*, Jan 2018, pp. 1–6.

[32] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Networks*, vol. 13, no. 1, pp. 27–59, Feb 2007.

[33] A. Abdul and S. Umar, "Attacks of Denial-of-Service on Networks Layer of OSI Model and Maintaining of Security," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 5, no. 1, pp. 181–186, 2017.

[34] S. De, C. Qiao, and H. Wu, "Meshed multipath routing with selective forwarding: an efficient strategy in wireless sensor networks," *Computer Networks*, vol. 43, no. 4, pp. 481 – 497, 2003.

[35] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, Energy-efficient Multipath Routing in Wireless Sensor Networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, no. 4, pp. 11–25, Oct. 2001.

[36] D. F. William A. Arbaugh, A. Keromytis and J. M. Smith, "Automated Recovery in a Secure Bootstrap Process," in *NDSS*, 1998, p. 155167.

[37] A.Herzberg and A.Gbara., "Trustbar:Protecting (even naive) web users from spoofing and phishing attacks," in *Cryptology ePrint Archive, Report 2004/155*, Oct 2004, pp. 1–9.

[38] B.Ross, C.Jackson, N.Miyake, D. Boneh, and J.Mitchell, "Stronger Password Authentication Using Browser Extensions," in *USENIX Security Symposium*, 2005.

[39] "Netcraft. netcraft anti-phishing tool bar." [Online]. Available: http://toolbar.netcraft.com/.

[40] R. Clayton, "Insecure Real-World Authentication Protocols (or why Phishing Is So Profitable)," in *International Workshop on Security Protocols*. Berlin, Heidelberg: Springer, 2007, pp. 82–88.

[41] "Microsoft delivers new tools to help reduce spam," in *Microsoft*, 2005. [Online]. Available: https://news.microsoft.com/2005/05/26/microsoft-delivers-new-tools-to-help-reduce-spam/

[42] C. Cowan, C. Pu, D. Maier, H. Hintony, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, and Q. Zhang, "Stackguard: Automatic Adaptive Detection and Prevention of Buffer-overflow Attacks," in *USENIX Security Symposium*, 1998, pp. 5–5.

[43] A. Baratloo, N. Singh, and T. Tsai, "Transparent Run-time Defense Against Stack Smashing Attacks," in *USENIX Annual Technical Conference*, 2000, pp. 21–21.

[44] M. Abomhara and G. M. Kien, "Security and privacy in the Internet of Things: Current status and open issues," in *PRISMS*, May 2014, pp. 1–8.

[45] H. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 4, pp. 337–340, Oct 2007.

[46] K. Park and H. Lee, "On the Effectiveness of Route-based Packet Filtering for Distributed DoS Attack Prevention in Power-law Internets," in *SIGCOMM*. ACM, 2001, pp. 15–26.

[47] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Advances in Cryptology — CRYPTO '96*, N. Koblitz, Ed., 1996.

[48] J. Choi and Y. Kim, "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system," in *APSIPA ASC*, Dec 2016, pp. 1–4.

[49] L. A. Tawalbeh and T. F. Somani, "More secure Internet of Things using robust encryption algorithms against side channel attacks," in *AICCSA*, Nov 2016, pp. 1–6.

[50] M. Wählisch, O. Maennel, and T. C. Schmidt, "Towards detecting bgp route hijacking using the rpki," in *ACM SIGCOMM*, ser. SIGCOMM '12, 2012, pp. 103–104.

[51] S. Y. Nam, D. Kim, and J. Kim, "Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks," *IEEE Communications Letters*, vol. 14, no. 2, pp. 187–189, February 2010.

[52] A. P. Ortega, X. E. Marcos, L. D. Chiang, and C. L. Abad, "Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt," in *LANOMS*, Oct 2009, pp. 1–9.