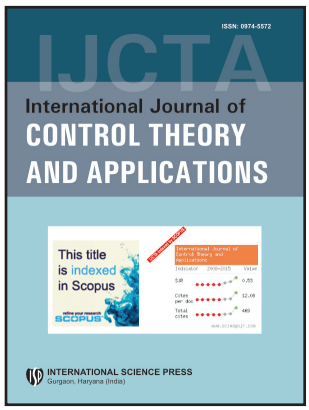

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 44 • 2016

Security Issues in Wireless Sensor Networks on an Internet of Things (IoT) Platform

Thirukkumaran.R[a] and Muthukannan.P[b]

[a]*Department of Electronics and Communication Engineering, Saveetha School of Engineering, Chennai, TamilNadu – 602105, India. Email: kumaran.satinfo@gmail.com*
[b]*Department of Electrical and Electronics Engineering, Saveetha School of Engineering, Chennai, TamilNadu – 602105, India. Email: pmkannan@gmail.com*

Abstract: The Internet of Things (IoT) is technological revolution that has recently become more important to the real world because of the growth of smart devices, embedded and ubiquitous communication technologies. The emerging field of Wireless Sensor Network (WSN) is a wireless network combines sensing, computation, and communication executed with spatially distributed autonomous small low power tiny devices to monitor physical or environmental conditions like Environmental/Habitat monitoring, Inventory tracking, Seismic Detection, Military surveillance, Acoustic detection, Smart spaces, Medical monitoring and Process Monitoring. More than billions of objects are interconnected over private or public network that can able to sense, share information and communicate through cloud services anywhere, anytime in IoT. Cloud network uses the internet as the communication media for providing different application, computing and storage infrastructure services for IoT enabled devices. However, security is one of the major factors that affect the large scale deployment and control of the sensor devices. If a Wireless Sensor Network is integrated into the IoT there will appear new security challenges. In an effort to understand the importance of security in IoT domain, this paper reviews the current research of various attacker model that impact the performance of WSN and cloud network.

Keywords: Security, WSN, Attacker, IoT, Cloud, Cryptography.

1. INTRODUCTION

Wireless Sensor Network having a large number of tiny sensor nodes, which are densely deployed in ad-hoc manner with one or more base stations. The number of nodes in a sensor network can higher than the nodes in an ad hoc network. Sensor devices are having limited capacity of power, computation and memory. Most cases sensors deployed in remote places that are easily prone to failures. In some application the topology of a sensor network changes frequently. Sensor nodes may not have global ID. WSNs have many applications [4], including military, target tracking, environmental monitoring, and healthcare, logistic and so on. Base station collects the data from all sensor nodes and store for analysis. If we hope to read the data and control the devices

from anywhere in the world, we need to integrate the WSNs into Cloud network as part of the IoT [7]. In order to connect WSN [3] to the part of IoT paradigm several challenges must be considered for security.

Cloud Computing is a method in which the internet is used as a medium to enable resource and application sharing. The Features of cloud computing are the internet-based services to support business process and rent IT services on a utility-like basis. It is the new infrastructure paradigm and has the characteristics of Ubiquitous network accessibility, Location independent distributed resource pooling, on demand self-service and rapid elasticity. It reduces the infrastructure management costs.

Inside the cloud network nothing is visible to the clients so clients have no idea or control over what happens inside a cloud. Even though the cloud provider is providing honest service, it can have malicious system admins who can tamper with the Virtual Machines (VM) and violate confidentiality and integrity. Clouds are still subject to traditional security issues like data confidentiality, integrity, availability, and privacy. Intruder or attackers can target the bandwidth and processing capacity of a cloud network.

Figure 1 shows the various attacking model affect the IoT enabled services classified in terms of cloud network and WSN. In WSN the most of the attacks are based on identity and in cloud network mostly on IP based.

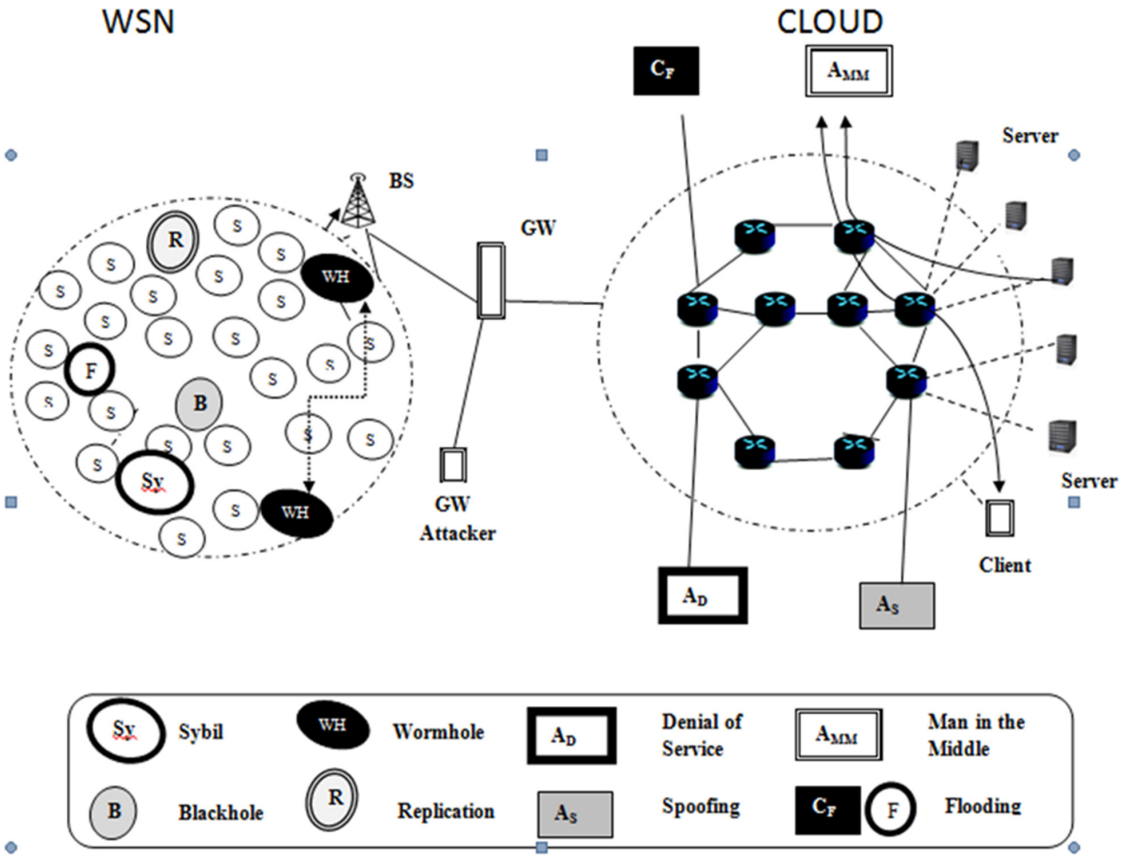

Figure 1: Attackers in WSN and Cloud Network

2. WSN ATTACKS

Any WSN that directly provides its services to external entities are quite vulnerable against attacks. To prevent such attack gateways and sensor nodes must include some efficient security mechanisms [2] that increase their robustness and defend these attacks. This section discuss about various attacks impact the WSN [18].

2.1. Sinkhole Attack

A malicious node uses the fault entry in a routing table to attract much traffic from a particular area, thus creating a sinkhole [8]. In the WSN sink node sends beacon message as broadcast throughout the network to update the routing table of all the sensor nodes to forward the data to sink node. Sinkhole attacker node while forwarding beacon message changes the hop count value as less to set this node as forwarding node i.e. next hop to reach sink node for remaining other nodes. During the data transmission each sensor node forwards the data to next hop nodes in the routing table. Once data is received by the sinkhole attacker drops the packet instead of forwarding. Sinkholes are difficult to defend because of its use highly quality communication link to fake a good quality route. It is difficult to defend.

2.2. Wormhole Attack

The wormhole attack performed by two malicious nodes placed in two different places in the network connected with wired or high power wireless connectivity termed as tunneling. The routing messages are forwarded or replayed form one part of network to another part of network by wormhole nodes with the help of low-latency tunneling link. During the route finding process one wormhole node forwards or replays the route request packet to the wormhole node in another part of the network. The path in wormhole nodes is selected as a shortest path between source node to destination. So that source node forwards the data through wormhole nodes. This is very difficult to detect when used in conjunction with Sybil attack or Spoofing attack.

2.3. Black-hole Attack

Black-hole [6] node is a malicious node that can attract all the packets, by sending route reply message with highest sequence number to falsely claiming a fresh route to the destination and then absorb them without forwarding data to the destination. Co-operative Black hole means the multiple malicious nodes jointly act together to collapse the entire network.

2.4. Replication Attack

In WSN environment all the sensor nodes are small, low-cost and usually hardware unprotected and many monitoring applications sensors are deployed remotely. Unshielded legitimated sensor nodes are easily to be captured and replicated with same ID in hostile environments by the adversary is called as node [5] replication attack. Replicated nodes are deployed in various part of the network to capture the data from other sensor and inject malicious data into the network.

2.5. Sybil Attack

The Sybil attack [16] is also a kind of replication attack instead of single identity it uses multiple identity. Adversary captures the multiple IDs from the network and use with replicated node. Multiple identities on same node leads routing misbehaviour and exploits identity based cryptography solutions. It affects the geographical routing protocol also.

2.6. Hello Flood Attack

Hello message[14] is one of the control message used to maintain network topology. In general each node broadcast hello message periodically to one hop neighbours. Which are the nodes are received hello message update neighbour table for maintaining one hop neighbour within the coverage area. An adversary node with

high transmission power floods the hello message at high rate. Adversary node becomes neighbour node to the normal nodes even though they are not in coverage. Due to flooding normal nodes cannot be access the channel at right time and wrong routing entries created in the routing table.

2.7. Acknowledgement (Ack) Spoofing

During the link-layer acknowledgement procedure, a malicious node forged the acknowledgement and shows the weak link as strong link and dead node as live node. Packets forward through this route may be dropped are get delayed.

2.8. Selective Forwarding

A malicious node can selectively drop or forward [1] packets. This kind of attacker node forward the data only from particular sensor nodes and the remaining data from other sources will be dropped. Due to selfish nature also the particular node may act as like selective forwarding [13].

3. CLOUD ATTACKS

Since cloud computing uses the Internet as the communication media for providing different computing services for IoT [10] [11] enabled devices, it is vulnerable to various network security threats. This section discuss about various network security threats that could occur on the cloud network.

3.1. Distributed Denial of Service (DDoS)

Distributed Denial of Service [9] attack is the most important considerable security threat in cloud service. DDOS is a large scale coordinated attack that causes the availability of the service in terms of Bandwidth and processing capacity. Many nodes are attacking one service or server simultaneously and continuously by sending flooding messages. The Cloud Service Provider (CSP) would need to detect and protect this kind of attacker. DDOS is distributed so we need co-operative protection technique should apply with multiple cloud service providers and Internet Service Providers (ISP).

3.2. Flooding Attack

A malicious node sends unwanted request or message to the particular service continuously. Each request is processed by the service to validate the request or provide some output the malicious node, it will increases the workload of the particular service. In cloud computing each service is limited with the server hardware resources. Once the server hardware resources are fully utilized by the flooding request legitimate user cannot access the particular service or other services running on the same server cannot perform their task. Flooding attack causes the Denial of Service (DoS) to the server hardware.

3.3. Cloud Malware Injection Attack

This kind of attack attempt to inject a malicious service implementation or virtual machine into the Cloud system. Such kind of Cloud malware [15] could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings. This attack requires the adversary to create its own malicious service implementation module or virtual machine instance, and add it to the cloud.

3.4. Side Channel Attack

This kind of attack [19] involves using timing information, power consumption, electromagnetic leaks or even sound to break the system.

3.5. Man In The Middle Attack

This kind of attack involves interception of traffic by being in the middle of the traffic flowing between the cloud and the intended recipient. Spoofed data is sent to both the endpoints.

3.6. Spoofing

This kind of data interception is done by sending illegitimate connection requests and messages from invalid sources. The scatter effect produced and utilized to produce further attacks on the cloud

3.7. Sniffer

This attack involves sniffing and manipulating packets flowing through the cloud network or between web browser and the cloud system.

3.8. Wrapping Attack

In this attack adversary node interrupt the client request and duplicate the body of Simple Object Application Protocol (SOAP) message during the Transport Layer Service (TLS) transaction and sent to the server as a legitimate user. The server validates the authentication through this duplicated signature and passes the message integrity check also. Now the adversary node can able to access the server in the cloud with the credentials of other node and can run malicious code to malfunction the servers.

3.9. Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a type of attack which target users website that accepts input used in scripts. In a vulnerable webpage attacker insert malicious code into user input field. The client browser loads the web page will execute the malicious script and allow the attacker to hijack the user session, redirect the user to a malicious website, view the paid content without payment, steal personal data and financial credentials. In the cloud environment distributed XSS attack also happen when XSS attack payload is injected in one web application but exposes its presence to another web application that can be very difficult to validate code form multiple sites. To protect this kind of attack update the web browser up-to-date and use it with latest XSS filters.

4. SECURITY CHALLENGES

The role of wireless infrastructure in IoT [17] applications is expected to become more prominent with the deployment of mobile nodes and wireless sensor networks. If the wireless sensor networks are being open to the internet connectivity, it becomes more vulnerable to attackers from anywhere in the world. Figure 2 shows the simple schematic of view of the security challenges due to various technologies that drive and move forward the IoT into next level and also it must be resolved simultaneously. The important challenges [2] are discussed here.

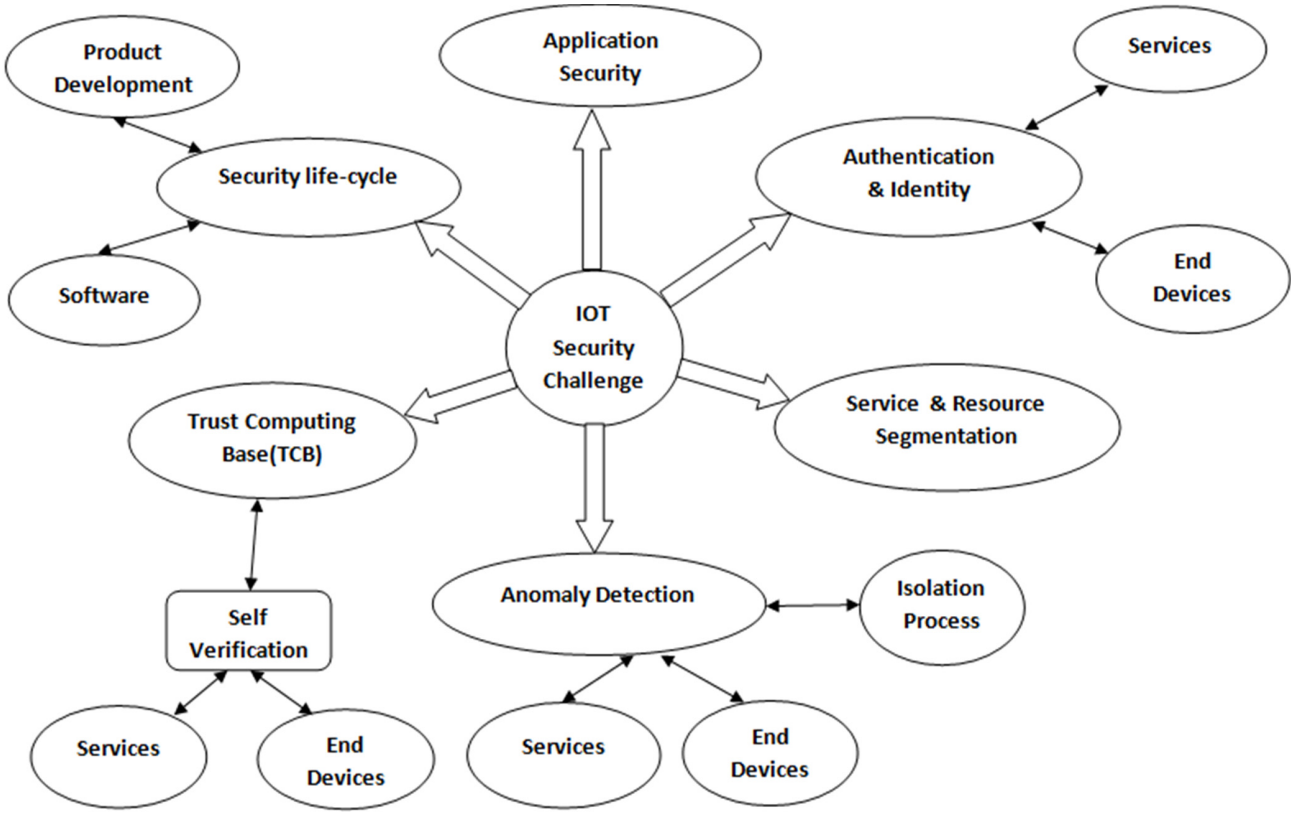

Figure 2: The Security Challenges

4.1. Availability

To achieve persistent connectivity between end point devices, users and their respective services new technologies to be designed. The power constrains of lightweight endpoints should be addressed in secure communication. Low Power Wide Area Network should be implemented with the same level of security used in recent mobile communication. During the migration of the IoT endpoints across network boundaries same level of security should be supported by the multiple mobile operators. Need to be address how the network trust can be forwarded from gateway to endpoints communication.

4.2. Identity

In an IoT product or service echo system Endpoint device should be securely identifying itself to its peers and services. This is critical and fundamental aspects to guarantee the data is being delivered to the certified peers and services. In IoT environment services and peers should verify the identity of the end-user and also endpoint device. Focusing security technology should be capable of securely authenticating peers and services. An Identity of a device should be secured from tampering and manipulation.

4.3. Privacy

Privacy must be designed to ensure that each and every action is authorized, device identity is verified and data are not exposed to unauthorized users. All the physical world entities are directly affected by digital world actions. It should be considered during the design of architecture of end point device or service.

4.4. Scalability

Scalability is defined as that increase in the number of nodes after the deployment of WSN. The expansion support of the networking protocol is a very important in the design of the protocol. The design of the services, protocols and end point devices should ensure that is scalable under varying load conditions.

4.5. Secure Routing

Routing [8] and data forwarding is an important service for allowing communication in wireless sensor networks and IoT. Existing routing protocols suffer from several security vulnerabilities. Information security practices must be enforced on both Endpoint devices and IoT Services through secure routing.

5. CONCLUSION

Every object in the WSN when connected to the internet, becoming part of the Internet of Things (IoT) and access the service through cloud network they must use same reliable protocol to ensure the interoperability and avoid vulnerabilities. Security perspective of WSN integrated to IoT [12] should concentrate standardization of protocols with ease of access and less overhead that supports integrity, end-to-end confidentiality, authentication and non repudiation services.

REFERENCES

[1] Alejandro Proano and LoukasLazos, "Packet-Hiding Methods for Preventing Selective Jamming Attacks" IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 1, January/February 2012.

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

[3] Fagen Li and Pan Xiong, "Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things" IEEE SENSORS JOURNAL, Vol. 13, No. 10, OCTOBER 2013.

[4] Farah Hussein Mohammed, Dr. RoslanEsmail, "Survey on IoT Services: Classifications and Applications" International Journal of Science and Research (IJSR), Volume 4 Issue 1, January 2015.

[5] Jae-Ho Choi, Kyu-Sun Shim, SangKeun Lee, and Kun-Lung Wu, Fellow, IEEE, "Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network" IEEE TRANSACTIONS ON MOBILE COMPUTING, Vol. 11, No. 2, FEBRUARY 2012.

[6] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, NingLIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network" IEEE International Conference on Advanced Information Networking and Applications, 24th, 2010.

[7] Li Da Xu, Wu He, ShancangLi, "Internet of Things in Industries: A Survey" IEEE, 2013.

[8] LipingTeng, Yongping Zhang, "SeRA: A Secure Routing Algorithm against Sinkhole Attacks for Mobile Wireless Sensor Networks" Second International Conference on Computer Modeling and Simulation, 2010.

[9] Mauro Conti, Member, IEEE, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, Member, IEEE, "Distributed Detection of Clone Attacks in Wireless Sensor Networks" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, Vol. 8, No. 5, SEPTEMBER/OCTOBER 2011.

[10] Ms. R. Sujitha, Mr. N. VijayaRaghavan, Ms. K. S. Suganya, Prof. A. Devipriya, "A Novel Survey On Internet Of Things Security And Its Application" IJAICT Volume 1, Issue 8, December 2014

[11] Omar Said &MehediMasud, "Towards Internet of Things: Survey and Future Vision" International Journal of Computer Networks (IJCN), Volume (5) : Issue (1) : 2013.

[12] PrajaktaPande, Anand R. Padwalkar, "Internet of Things –A Future of Internet: A Survey" International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 2, February 2014.

[13] PreetiSharma, MonikaSaluja and Krishan Kumar Saluja, Francisco Vazquez-Gallego, Jesus Alonso-Zarate, "A Review of Selective Forwarding Attacks in Wireless Sensor Networks" International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.3, July 2012.

[14] Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE"Mitigating Routing Misbehavior in Disruption Tolerant Networks"IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol. 7, No. 2, APRIL 2012.

[15] Shikha Singh, Binay Kumar Pandey, RatneshSrivastava, Neharawat, Poonamrawat, Awantika, "Cloud Computing Attacks: A Discussion With Solutions" Open Journal of Mobile Computing and Cloud Computing Volum1, Number1, Aug2014.

[16] Sohail Abbas, MadjidMerabti, David Llewellyn-Jones, and KashifKifayat, "Lightweight Sybil Attack Detection in MANETs" IEEE SYSTEMS JOURNAL, Vol. 7, No. 2, JUNE 2013.

[17] SyeLoongKeoh, Sandeep S. Kumar, and HannesTschofenig, "Securing the Internet of Things: A Standardization Perspective"IEEE INTERNET OF THINGS JOURNAL, Vol. 1, No. 3, JUNE 2014.

[18] VasileiosKaragiannis, PeriklisChatzimisios, Francisco Vazquez-Gallego, Jesus Alonso-Zarate, "A Survey on Application Layer Protocols for the Internet of Things" Transaction on IoT and Cloud Computing 2015.

[19] YANG Jin-cui, FANG Bin-xing"Security model and key technologies for the Internet of things"The Journal of China Universities of Posts and Telecommunications, December 2011.