IoT Operating Systems and Security Challenges

Muhammad Asim

National University of Science and Technology (NUST), Islamabad, Pakistan

Waseem Iqbal

National University of Science and Technology (NUST), Islamabad, Pakistan

***Abstract*— The emerging trend of pervasive computing aims embedded devices such as smart phones, autofocus cameras, musical instruments, home video systems etc with microprocessor and wireless communication capability. This type of computing paradigm is known as IoT (Internet of Things). IoT connects myriad of things for providing service to machines and humans. In 2020 it is expected billions of things in IoT will be deployed worldwide. Centralized computing approach does not provide sustainable model, so a new architecture is needed as trusted platform for expansion of Internet of Things (IoT). Data gather with IoT are often unstructured and noisy, so more computation power require for analysis and getting efficient results and also needed efficient mechanism for authentication in lightweight devices like IoT where less computation power, limited resources, low memory and low battery life.**

This paper is about operating systems of IoT and current security challenges in IoT using RPL and 6LoWPAN (IPv6 over low-power WPAN) protocols and also we will discuss possible solutions related to IoT Security challenges.

***Keywords*-- Wireless Sensor Network, Low power Wireless Personal Area Networks, Software Define Network.**

I. INTRODUCTION

IoT environment is based on the wireless sensors and it's applications, which makes regular operating system meaningless due to IoT low resources and computation power, in such situation development of lightweight operating system was necessary to meet resource constraint demand of internet of things (IoT).

There are different OS for IoT Environment such as Mbed, RIOT, Contiki, FreeRTOS etc. these all operating systems are well equipped with key communication and networking protocols, and security features but there is some implementation flaws or some protocol flaw which make network vulnerable to various kind of attack such as denial of service, fragmentation attacks, Black hole attack etc. we will discuss security issues of RPL and 6LoWAPN in next sections.

In this paper we will discuss different operating system for Internet of things in section II , in section III we will discuss RPL and various kind of attacks in RPL and recommend solution for improving security issues, in Section IV we will discuss 6LoWPAN and some security issues related 6LoWPAN. In section V we will discuss SDN based architecture for IoT, Conclusion of this paper is in section VI.

II. OS FOR IOT ENVIRONMENT

Integration of various IoT to various objects are possible through software along with WSN (Wireless Sensor Network) and RFID technologies. Interactions with these objects or devices are possible through OS. With flexible features of operating systems makes IoT easier to use. The operating system for IoT needs few kilobytes of memory and operates on low power consumption. This operating system doesn't compromise in features such as networking, security, communication etc as in traditional Operating systems like Windows, Linux etc. Operating system for IoT having number of unique security features to avoid compromise of usability and stability of the operating system. Operating systems for IoT environment due to security issue are quite different as compare to regular operating system. in IoT environment information is exchange between various devices the most efficient way is to use low amount of resources. OS and IoT environment is prone to third party attacks. Encryption, intrusion detection [1] and data hiding techniques [2] have paramount importance in IoT infrastructure.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

A. Mbed:

Mbed is operating system develop by ARM with collaboration of technological partners, it is 32 bit ARM Cortex M Microcontroller, this OS is written in C++ and C language and Open source under Apache License 2.0. SDK for mbed offers framework for developing various firmwares for IoT devices. The Core libraries consist of following components:

1. Networking
2. Test scripts
3. RTOS and runtime environment
4. Build tools
5. Debug Scripts
6. Microcontroller peripheral drivers

Mbed application are develop online using mbed online IDEs (integrated development environments), code can be written only in web browser and ARMCC C++ / C is complier. Mbed supports following technologies:

1. Bluetooth
2. Wifi
3. Zigbee IP / LAN
4. Cellular
5. 6LoWPAN

Mbed provides (IPv4 and IPv6) E2E security through DTLS and TLS, OMA lightweight protocol use for management in this environment.

B. RIOT

RIOT is compatible with AVR Atmega, TI MSP430 and ARM Cortex-M3/M4, this is also open source under LGPL V2.1 licensed and develop in C++ and C. SDK for RIOT OS are gdb, valgrind and gcc. RIOT support following networking and communication protocols:

1. IPv6
2. 6LoWPAN
3. RPL
4. CoAP
5. UDP
6. TCP
7. CBOR
8. CCN-lite
9. OpenWSN
10. UBJSON

C. Contiki:

Developed by Adam Dunkels and then revised by various organizations like Cisco, SAP, Atmel, Sensinod etc[3]. It supports various microcontroller devices such as Atmel ARM, Atmel AVR, STM32w,TIMSP430 /CC2430 /CC2538 /CC2630 /CC2650, LPC2103, Freescale MC13224, Microchip dsPIC, Mirochip PIC32. Contiki is also open source under BSD license, it has features of contiki nodes simulation, supports three types of nodes: Emulated , Cooja and java nodes and supports CoAP, 6LoWPAN and RPL networking protocols. Contiki is secure with implementation of DTLS/TLS and ContikiSec [4].

D. TinyOS:

TinyOs is Open source developed by TinyOS-Alliance for wireless sensor networks written in nesC under BSD license. SDK for TinyOS are combination of TinyDT, TinyOS Eclipse Plugin – YETI 2 and Eclips Editor plugin. TinyOS supports Broadcast based Routing, Multi-Path Routing, Geographical Routing, Routing Reliability based , TDMA base Routing. TinySec made TinyOS architecture Secure [5].

III. RPL (Routing Protocol for Low Power and Lossy Network)

RPL (Routing Protocol for Low Power and lossy network). Aim of RPL is to communicate multipoint to point also supports P2M (point to multi-point) and P2P (point to point) communications. RPL Topology contains 1 root known as sink node. RPL form Destination Oriented Directed Acyclic Graph tree structure. Topology formations start with root node broadcasting DODAG information object (DIO). Rank value is calculated with respect to PRV (parent rank value) and some other parameters when any node receive DIO message. RV also depended on distance between root node and Parent note and also link energy. RV calculation parameters are decided by the network owner.

Devices are mostly resource constrained, IoT devices are house hold appliances, smart meters, sensor nodes etc. hundreds of devices are available which can connect to IoT. 6LoWPAN allows constrained devices to communicate with IPv6 network. 6LoWPAN is compression protocol which can be easily attack. IoT devices are limited in resources, so new protocol is design for network

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

routing called RPL. RPL don't having routing like traditional routing protocol.

In [6] discuss different types of attacks in RPL and possible solutions such as selective forwarding attack, we will go step further and discuss about Internet Smurf attack, Black hole attack detection, Homing attack, Wormhole attack detection, Sybil and Clone ID attack detection, Sinkhole attack detection, Resource Exhausting attack and RPL attack.

A. Smurf Attack

Smurf attack causes DoS in network makes network untreatable. To address vulnerabilities first we should understand basics of ICMP (Internet Control Message Protocol). ICMP control network nodes and information of ICMP can be change by network administrator. It is also use to monitor status of other IoT nodes. If it returns ping then this means they are operating. [7] To prevent from this type of attack, configure OS in PaaS layer and router in IaaS layer.

B. Black hole Attack

HCP (heterogeneous communication protocols) are vulnerable to different kind of attacks like network sniffing, modification, Dos etc. some types of attack are documented in [8]. Black hole attack is on network layer, this target RPL implementation of contiki operating system. Author demonstrated this attack in [9], black hole attack start with compromised node which act like malicious and drop packet which are routed through it and cause disruptions in network data flow. Black hole attack can be easily concealed and attacked network may be behaved like health network. It is very important to know that only contikiOS based devices are vulnerable to this kind of attack. best defense against black hole attack in RTL protocol is to implement RIOT OS, Tiny OS which are not vulnerable to this kind of attack.

C. Wormhole attack detection

In [10] author describe how to detect worm hole attack in wireless network. Worm hole attack causing serous damage to nodes and network. To prevent form such kind of attack we use special timer WAPT, using timer nodes don't need to synchronize their clock, when a node send RREQ packet. It will travels from one node to another and then back. If WAPT is large then it is very difficult to detect. For sensor nodes WAPT is:

WAPT = 2 * Transmission Range / Propagation Speed of packet

Monitor neighbour node for hidden attack detection. If wormhole nodes are as a legitimate node then it is very difficult to detect by only monitoring mechanism. In ad hoc network wormhole detection is still big challenging.

D. The Sybil Attack

RPL protocol is vulnerable to Sybil attacks, Sybil attack is when a single malicious identity can show multiple identity and gain control of network. WSNs are vulnerable to various attacks like nodes compromising, replay attack etc, mostly these attack are deal with cryptographic protocols and key management schemes. Sybil attack is significant attack in WSNs, in Sybil attack the attacker compromise or capture several nodes, to conduct other attacks it inject compromise nodes throughout network. These nodes cause consuming large amount of resources. To prevent or check integrity ELgamal key management can be use. In [11] author describes how to prevent over WSNs network form Sybil attack.

E. Clone ID Attack

In RPL Network Clone ID attacks are possible [12]. In this attack, attacker nodes clone identity of another. These attacks are minimized with tracking no of every identity. In case of geographical location nodes identify store in 6BR, by using this we can recognize clone or original node.

F. Hello Flooding Attack

Network initially broadcast HELLO message, attacker can show himself as neighbor node and broadcast HELLO message to enter in network with strong routing metrics. This attack can be avoid by using link layer metric in default route [13]. Other solution of this attack is to use geographical distance. Due to RPL's Local and Global repair mechanism this attack cannot exist for long time. If multiple attacker combine then RPL's Local and Global repair cannot remove it.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

IV. 6LoWPAN

6LoWPAN infrastructure is IP-Based and WSNs specify IPv6 packet routing in networks like IEEE 802.15.4. 6LoWPAN defines reassembly of datagram and fragmentation due to link layer limited payload size. 6LoWPAN connect with internet with 6LoWPAN Border Router, that perform fragmentation, decompression and compression of IPv6 datagram's. Following are attacks on 6LoWPAN.

A. Fragmentation Attack

We connect devices with IPv6 network with 6LoWPAN protocol. In IPv6 fragmentation is done because of Minimum size of IPv6 MTU is 1280 bytes while nodes in IoT or sensors having maximum 127 bytes MTU. Another reason of fragmentation attack is 6LoWPAN does not support authentication. Due to no authentication in 6LoWPAN, an attack can put own fragment in fragmentation chain. To check that fragment chain is not spoofed the author proposed two mechanisms [14]. One is split buffer approach promote competition between reassembly buffer resource and the original sender, another is the content chaining, cryptographic approach is used to verify the fragment in of same packet or not.

B. Confidentiality Attack

6LoWPAN provide secure communication end to end between traditional network and IP based sensor. Due to encryption in 6LoWPAN helps in mitigation various attacks such as spoofing, eavesdropping and Man in middle etc. it supports both encapsulation Security Payload and IPSec's Authentication Header. For encrypting packets faster Crypto hardware are used for 6LoWPAN with in IEEE 802.15.4 [15].In [16] author examined MT6D (Moving Target IPv6 Defence) in 6LoWPAN. Nodes change their address continuously in MT6D and attacker will not be able to attack on specific sensor or node. Aim of MT6D is to defend network against DoS and Man in The Middle attacks.

C. Authentication Attack

6LoWPAN doesn't provide any authentication mechanism for nodes when joining to the network. Because of this any malicious node can join. For authentication mechanism author describe in [17] for controlling nodes having access to the 6LoWPAN network. This is based on the administrative approval. This is comprises of four steps: node authorization, data filtering, authorized node list propagation and node presence detection. List of all nodes with layer 2 address are save in border router, with the help of these address presence of node is determined and also allow only those nodes to connect with network with are in list. For data filtering and flow of data between nodes these list also used.

V. SDN BASED ARCHITECTURE FOR IoT

Traditional equipments and protocols support high amount of traffic, scalability and mobility. In [18] author proposed IoT architecture. Beside this research we will discuss about SDN architecture.

In IoT networks or sensor networks, each device is not compatible to SDN controller or SDN embedding compatibility. If we assume that every node in IoT having less resources is connected with SDN Capability nodes. Now in this domain we have two types of nodes. One is OF which having enough resources and second one is smart object or sensor which having not enough resources. SDN control all traffic in this domain. In this architecture multiple SDN domains, each domain have at least one SDN controller. SDN are not only use for managing network but it provide efficient security against inside and outside attacks. First we will explain security of one controller manager in one SDN. To secure network resources the SDN authenticate network devices, once secure connection established between controller and switch, then block all ports which are directly connected with users. We can extend this process to each device, each node connected with OpenFlow and one of the node is connected with one domain controller [19].

VI. Conclusion

From the above research we conclude that Mostly IoT operating systems are well organized and flexible, but there are some protocols or implementation problem due to which over networks are vulnerable to different kind of attacks. So far various techniques are proposed against

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

6LoWPAN and RPL attacks, still there are many kind of attacks which are not evaluated, needed more research to counter weakness of 6LoWPAN and RPL. Clone ID, Black hole , wormhole , Sybil etc such kind of attacks need IDS based detection mechanism.

REFERENCES

[1] Manoj Rameshchandra Thakur, and Sugata Sanyal. "A Multi-Dimensional approach towards Intrusion Detection System." arXiv preprint arXiv: 1205.2340(2012).

[2] Harshavardhan Kayarkar, and Sugata Sanyal. "A survey on various data hiding techniques and their comparative analysis." arXiv preprint arXiv: 1206.1957(2012).

[3] Adam Dunkels, Oliver Schmidt, Niclas Finne, Joakim Eriksson, Fredrik Österlind, Nicolas Tsiftes and Mathilde Durvy. "The Contiki OS: The Operating System for the Internet of Things." (2011).

[4] Vladislav Perelman. "Security in IPv6-enabled wireless sensor networks: An implementation of TLS/DTLS for the Contiki operating system." PhD diss., MSc Thesis, Jacobs University Bremen, 2012.

[5] Kresimir Grgic, Drago Zagar, and Visnja Krizanovic. "Security in IPv6-based wireless sensor network—Precision agriculture example." In Telecommunications (ConTEL), 2013 12th International Conference on, pp. 79-86. IEEE, 2013.

[6] Pava Pongle and Gurunath Chavan. "A Survey: Attacks on RPL and 6LoWPAN in IoT", International Conference on Pervasive Computing (ICPC) 2015.

[7] Niraj Suresh Katkamwar, Atharva Girish Puranik and Purva Deshpande, "Securing cloud servers against flooding based DDoS attacks", International journal of application or innovation in engineering and management, vol.1, issue 3, November 2012.

[8] Changmin Lee_, Luca Zappaterra_, Kwanghee Choi_y, and Hyeong-Ah Choi, "Securing Smart Home: Technologies, Security Challenges, and Security Requirements", *IEEE Conference on Communications and Network Security (CNS), 2014.*

[9] K. Chugh, A. Lasebae, and J. Loo, "Case study of a black hole attack on 6lowpan-rpl," in SECURWARE, *The Sixth International Conference on Emerging Security Information, Systems and Technologies*, pp. 157– 162, 2012.

[10] Juhi Biswas, Ajay Gupta and Dayashankar Singh, "WADP: A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol", *9th International Conference on Industrial and Information Systems (ICIIS), 2014.*

[11] S.Krishna Kumar ,V.Shalini , V.Shiva and P.Vijayakanth, "Detection And Prevention Of Sybil Attack Using A Thershold Elgamal Key Management Scheme", *International Journal of Advances in Engineerin*,1(3), 319 – 322, 2015.

[12] Wallgren, Linus, Shahid Raza, and Thiemo Voigt. "Routing Attacks and Countermeasures in the RPL-based Internet of Things." *International Journal of Distributed Sensor Networks 2013* (2013).

[13] Le, Anhtuan, et al. "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks." (2013): 1-1. (2013)

[14] Hummen, René, et al. "6LoWPAN fragmentation attacks and mitigation mechanisms." *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks. ACM*, 2013.

[15] Raza, Shahid, et al. "Secure communication for the Internet of Things—a comparison of link layer security and IPsec for 6LoWPAN." *Security and Communication Networks* (2012).

[16] Sherburne, Matthew, Randy Marchany, and Joseph Tront. "Implementing moving target IPv6 defense to secure 6LoWPAN in the internet of things and smart grid." *Proceedings of the 9th Annual Cyber and Information Security Research Conference. ACM*, 2014.

[17] Oliveira, Luis ML, et al. "Network admission control solution for 6LoWPAN networks." *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on. IEEE*, 2013.

[18] P. Diogo and L.P. Reis and N. Vasco Lopes, Internet of Things: *A system's architecture proposal, in 9th Iberian Conference on Information Systems and Technologies (CISTI)*, 2014 , pp.1,6, 18-21 June 2014

[19] Olivier FLAUZAC and Carlos GONZA´ LEZ and Abdelhak HACHANI and Florent NOLOT, "SDN based architecture for IoT and improvement of the security", *29th International Conference on Advanced Information Networking and Applications Workshops*, 2015

[20] Shradha Jain and Ashok Kajal, "Effective Analysis Of Risks And Vulnerabilities In Internet Of Things", *International Journal of Computing and Corporate Research*, 2015.