International Journal of Engineering & Technology, 7 (2.8) (2018) 261-267

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

An approach towards preventing iot based sybil attack based on contiki framework through cooja simulator

Prateek Singhal*, Puneet Sharma, Deepak Arora

Department of Computer Science and Engineering, Amity University,Uttar Pradesh, India
**Corresponding author E-mail: prateeksinghal2031@gmail.com*

Abstract

In this paper we propagate the Sybil attack in WSN (Wireless sensor network), by the researchers many attacks have been recognized in WSN till now and there are many attacks which can attack over through internet, Internet of thing means all devices is interconnected to each other M2M over internet and can be attacked by any of the attacker on any devices. Sybil attack is the detrimental attack against sensor network where several counterfeit identities and legitimate identities are used to get prohibited pass in a network. This is major attack which results an information loss and misinterpretation in the network, and it also minimizes the routing disturbance, trustworthiness and dropping sensitivity packets into a network. In this instance node can trust the imaginary node and sharing of information starts, owed to this security of node is get affected and information is lost. In this paper, a survey of CONTIKI OS-2.7, stimulation tool COOJA and the Sybil attack and proposed the defense mechanisms and CAM (Compare and Match) approach to verify the Sybil attack position and prevent it. This Sybil attack can be stimulated on the stimulation tool COOJA which helps to identify the attacker position node, whereas these attacks outcome in uni-casting as well as multicasting and in this paper specifically given the secure security for Wireless sensor network.

Keywords: *Sybil attack, Internet of Things; Wireless sensor network; CAM; Defense Mechanisms.*

1. Introduction

In past, few decades internet has become the most popular, while we talk about the increasing the internet connection or transferring the data packets to the portable devices and son on. User's increases which are directly proportional to each other to connect with the network. Whereas the cost of the connection is being decreased due to of the WIFI connectivity where the maximum number of devices is connected through a common medium. The technology so called Internet of Thing is introduced to fulfill the criteria and requirement of interconnection of internets. The Internet of Things was firstly introduced by Kelvin Asthon at 1999 in MIT lab science center and supply chain management [4]. Internet of Thing is an interconnection of network routine objects which are available with ubiquitous intelligence [1]. IoT is an evolving technology which helps us to connect a huge number of smart computing objects with physical as well as cyber globes through the internet and kept all the equipment's in a full connectivity without any uninterrupted interaction.

A lot of attention on WSN (Wireless sensor network) due to their promising and interesting function functionalities including location based services and mobile safety congestion avoidance [38]. In the today's research the topology creation and implementation of WSN has become very fast and growing rapidly. Application has blowout all over the fields from health, military, education, monitoring [39], whereas applications of WSN has become the most important because it provide security, prevention from attacks, perceiving from low level to high level attacks which is vulnerable to malicious attacks in wireless sensor network, hence erudite firewall system, powerful IDS are available [40]. Diversity of attacks is available such as black hole,

SYBIL, DDOS and selective forward attack which are present in the network. In the paradigms of security and privacy term in the internet of things, nowadays there are increasing the vulnerabilities in a web application which is exploited by the attackers and man-in-middle attacks which gave the unauthorized access to the data or information of web site or any private data. As per the new web system which is complex, distributed and heterogeneous, interactive and responsive, and rapidly changing [2]. Malevolent action like threats, virus attacks, security breaches, etc. are being made by the dynamic nature and pervasive in web domains. If we enlighten the web application in the IoT security becomes the more important and critical issue in it. There is a harmful attack known as SYBIL ATTACK which held on the network layer which works as the duplication of IDs with the original IDs means in this attack there are the fake IDs of the original nodes. There is an attacker which attacks the various nodes as a different IDs, but the attacker is the same. In simple words, we can say it is a spoofing of the nodes as different IDs which work on the Peer-to-Peer system by creating Pseudonymous. There is various Operating System is being used for the simulation or the emulation of the attacks where we can see the attacker breach, so we are using the latest OS which can directly emulator on the hardware that is [5] CONTIKI Operating System and the Tools is COOJA. This is the IoT tools which are more stable and directly implemented on the hardware with accuracy; COOJA is based on the C language for the implementation [6]. CONTIKI OS bring the IP to the networks means the new version of IPv6 from IPv4 where in IPv6 there is no shortage of any unique address it is

128bit addresses which is more than enough for all the devices and they can have a unique address to specify the devices.

A. Internet of Things

The word Internet of Things made the world available on the networks where the objects or entities that around us will directly or indirectly be connected to each other or available to us. Various sensors networks are being generated to share the information or data with each other but to connect with IoT RFID (radio frequency identification) is the best technologies whereas there are more technologies like ZigBee, 6LowPAN, z-wave, etc. [3]. IoT is the system of interrelated of physical network or computing devices where the physical as well as the objects are interlinked to each other which provides the unique identity to all and transfer data or information over a network over long ranges without requiring human-to-human or human-to-computer integration [7-8].

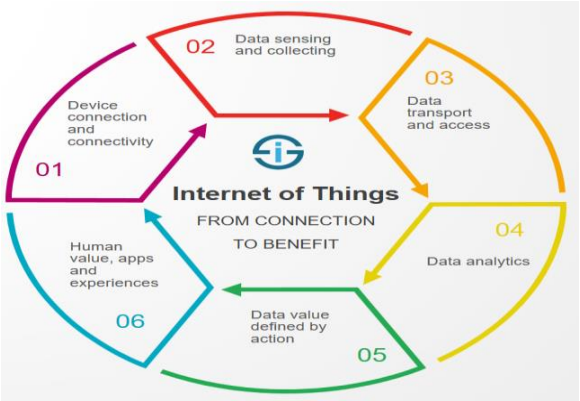

Fig. 1: Internet of Things

B. Sybil Attack

SYBIL attack is one of the detrimental attacks in WSN whereas it is named on the book "SYBIL" which is based on the case study of a woman who has a personality disorder and lives in United State. This is given by Brain zill working in Microsoft research labs [26]. It is becoming server problem in many areas such as voting system, fake IP are created to cast a vote and used to link the result of searches to the terms searched for political usages for advantage. If we talk about Ad- hoc network like MANET, there is a lack of centralized authority, Sybil node can misinform the honest nodes resulting into capture the nodes [29]. The network faces various security challenges whether security is being provided because, WSN are prone to the passive and active attacks. There is the large ratio for the acceptance of fake identity account is made [30].

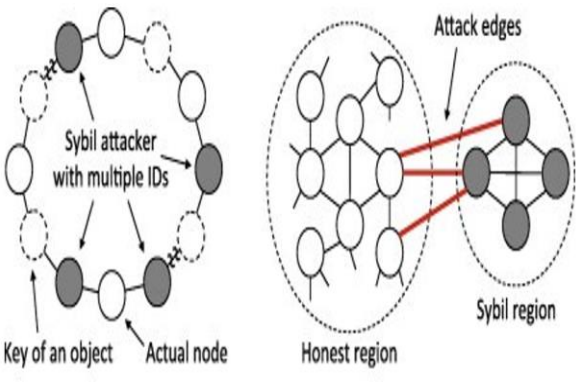

Fig. 2: Sybil Attack

There are many solutions has been developing to detect the SYBIL attacks such as Sybil guard, Sybil limit for he social networking [30-31], watchdogs and path rater in ad-hoc network also RSSI and channel based detection for WSN [32-33]. There are defenses mechanisms are developed in order to overcome the Sybil attack which includes Trusted certification [34], Votetrust [35], Sybil defender [36], Sybil limit [31]. There are various advantages and disadvantages where we talk about advantage schemes they are very effective, and they can be modified to improve the performance of algorithm. Disadvantage schemes they can be costlier, or they based on the model which themselves are vulnerable to attack.

2. Literature Review

J. Dalfiah [19] et al proposed the energy efficient integration of IDS (intrusion detection system) which detect the network layer SYBIL attack. In this it spots the node accurately and eliminates the false node which is behaving like an original node. The alternative proposed method is also a detection of malicious node accurately with spending the less energy relatively. T. G. Dhanalakshmi [20] et al explain the wireless sensors grids protection whereas various attacks have been recognized by the researches till now, but the most harmful attack is SYBIL ATTACK in the against of sensors grid where appropriate individual and fake individual are used to get the entry into the network inappropriately. To secure the data the author projected the technique to avoid the SYBIL attack which is common RAI (relate and identify tactic) and LVT (location verification technique). M. S. Khalil [21] et al proposed E-BIOSARP it is the enhancement of BIOSARP which is based on the random key encryption and decryption mechanisms to secure the data. X. Zhenghong [22] et al it explains the simulation result of the proposed protocol which can be detected and defend against routing attacks like SYBIL attack, WHORMHOLE attack and HELLO attack sophisticatedly. R. Vamsi [23] proposed a Lightweight SYBIL Attack Detection Framework (LSDF). The framework is alienated into two, first, evidence collection and second, evidence validation, where every node is collecting the evidence of neighboring nodes by observing the activity of it and it can validate by progressive hypothesis to decide neighboring node is a SYBIL NODE or benign node. When the wide simulation is being done, it revealed that LSDF with few evidences can perceive the SYBIL attack action accurately. Makhdoom [24] et al it gives a detailed review and analysis on the several defenses which was proposed against SYBIL attack. As the author know the weakness and strength and it gives a novel "One Way Code Attestation Protocol (OWCAP)" for wireless sensor networks. It is normal and economical secure code attestation which protect from SYBIL attack but also in contradiction of most of the insider attacks. Y. Sun [25] et al proposed the regional statistic detection (RSDs) which is against the SYBIL attack and it gives the effective solution key issues: firstly, by the RSSI-based distribution mechanism it has the address of SYBIL attack, Secondly, it prevent the network from large number of node failure which is caused by the SYBIL attack, Thirdly, it can say that by the help of implemented experiment it can be maintain the high detection probability with low system overheads which is being verified by the RSDs.

3. Architecture of IoT

IoT serene of two words i.e. "Internet" known an interconnection of networks and "things" known the object. When we put these words together, it means the World Wide Web networks of interconnected objects, addresses and communication protocols [9]. Security system which gives the terminal module, perception module and trusted network module. Generally, IoT is alienated into three layers: perception layer, network layer and application layer [10-11].

Perception Layer

At this layer, it helps us to collect the information from different devices, like RFID, smart car and sensor network. It has an inclusive sensing to get the object information through RFID system anywhere and anytime. Each RFID electronic tags has a unique id which is known as the electronic product code (EPC) it helps us to search the product with allotted id of each physical objects [12].

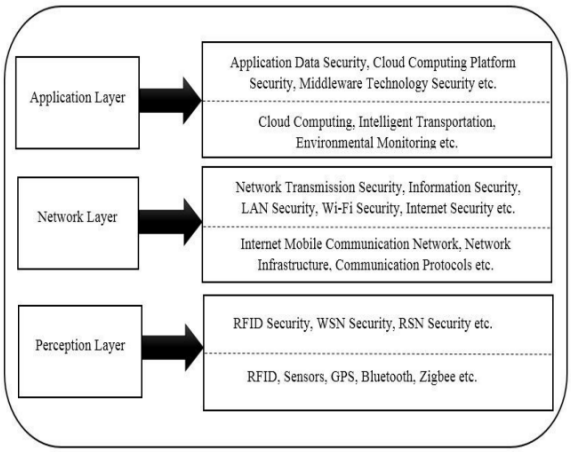

Fig. 3: IoT Architecture

Network Layer

The data is being gathered by the sensors and it transfer through internet over network layer with the help of computers and other components. Hence this layer is accountable for the transmission of information with reliable delivery and it includes the functionality of transport layer.

Application Layer

In this layer, received information is analyzed and control decision is made to achieve the feature of intelligent processing by interconnecting to a network which identify and control between devices and objects. The astuteness technology is cloud computing which process data for intelligent control such as what to do and when to do. Whereas this layer is also termed as process layer.

Security of IoT

As we know while transferring the data over network via internet is always a risk of attackers such as breaches, man-in-middle, etc. but we must have the security to prevent the data while we are exchanging the information. There are various security issues in the different layer where we can secure the data by various techniques.

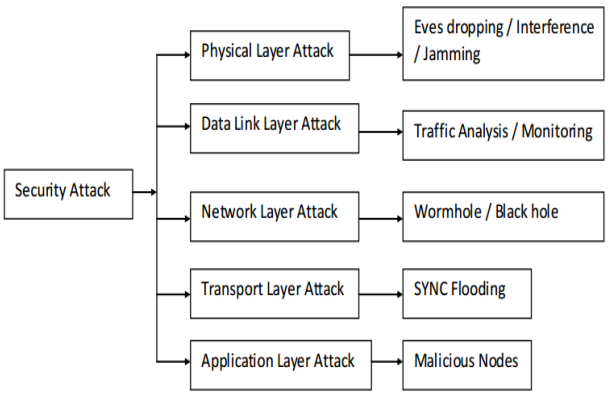

Fig. 4: Classification of Attacks

Security Issues in Layers

As the IoT system is rapidly increasing there should be a powerful protection against all the vulnerabilities. Each layer consists of various devices, application or networks, etc.

Security in Perception Layer

Where as in this layer in mainly includes the smart cards, RFID tags, sensors networks and these leads to a vulnerability in IoT devices such as radio interference, sensor attackers and sensor abnormalities [13].

Terminal security issues [10]: There is huge number of terminals, whereas terminals are being used to collect the information from the user which is presented in the real-time and needed a proper authentication and data integrity. The main problem it includes the leakage of confidential and private information, terminal virus, tampering and duplication of files, etc.

Sensor network security issues [10]: Data transmission, integration, data acquisition and collaboration are depending on the sensor nodes as they have less security protection, so it faces more complex issues as follows: -

Malicious code: Worm attack does not involve any sponging file and it can easily affect the wireless sensor networks, hence it is difficult to detect the codes.

Tags defects: It is not possible to provide enough security due to limited cost of tag which leads to illegal use of legal readers by this attacker we can easily get the information by RFID system is accessed illegally without any authentication thus, any rewritable tag can be decoded, fabricated or copied by the attackers.

Security in Network Layer

Primarily security issues include network content security, illegal authorization, hacker intrusion in the computers, wireless/wired networks [15].

Data transmission security issues: The data should be transfer securely so there are two main types in this layer: first risks of security in IoT itself; second during design and implementation there is defects related to protocol and technologies [10]. These nodes which can join and leave the network at any time without any preceding authentication and it can make the network more malicious for security.

Various attacks in this layer: Some risk which is faced in the network layer such as confidentiality, data eavesdropping, virus attack, destruction, illegal access, DOS attack, man-in-middle attack and so on.

SYBIL attack: Attack where the multiple identities are being presented to the other nodes, but it is a replication of a single node and it is basically a spoofing of the nodes IDs.

WORMHOLE attack: Attack where the bits of data are being relocated from its original position and relocation of data packet is carried out when the bits of data is passes over a link of low latency.

Security in Application Layer

The intelligent devices are included for the effective decision making and vulnerability which lead to an issue of security in IoT.

Application safety issues: The main security problem is its own design flaws which attract the attacker to attack on it, whereas the software vulnerabilities and malicious code is introduced as a defected system. Varity of application are monitoring service, smart grid, industrial monitoring and the intelligent systems. The other issues need to be integrated which causes a blockage for the huge data processing and operation control [16] which lead to security issues of reliability and safety for Internet of Things (IoT). Some of the issue that can have privacy protection technology such as database access control, information leakage technology, securing electronic products technology and the intellectual property of software [17].

Security Challenges in Network

Now-a-days researchers concern the security as a primary. There are many security mechanisms with some specific assumption which are vulnerable to serve attack whereas while building security mechanisms all security challenges should be considered. Some as follows:

- Passive and active attack: The identities of the nodes are stolen, and detection of honest nodes becomes challenging task.
- Energy consideration in WSN: It plays important role as node has limited energy in which task is to be completed.

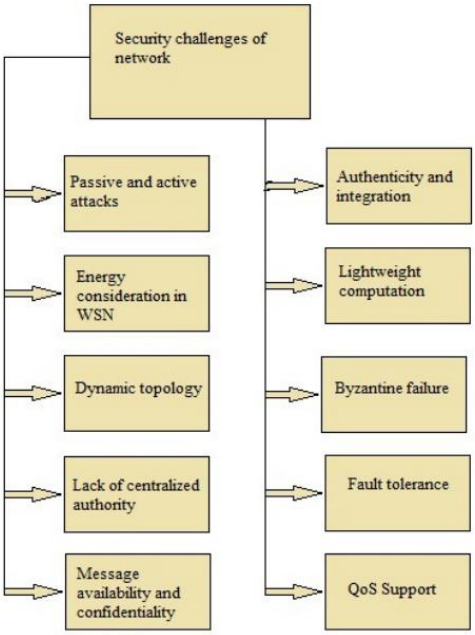

Fig. 5: Security Challenges of Network

- Dynamic topology: It is also a security challenge for detecting the attack nodes.
- Lack of centralized authority: In some of the networks the CA is absent which lead to disturb in the mechanisms for detecting the Sybil attack.
- Message availability and confidentiality: message should be available and confidential at the same time. Losses of confidentiality which may lead the network interrupt to the attack.
- Authenticity and integration: Integrity should be provided to the message so it should not be altered by the attacker.
- Lightweight computation: lightweight computation should be built in order to make the mechanisms time efficient and cost effective.
- Byzantine failure: nodes take participation in routing which may lead to the disrupted by an attacker, causes unrecoverable failure to the network.
- Fault tolerance: the defence mechanisms should be strong enough to face the faults in the networks.

Critical IoT Security Technologies for Attack

In the security technologies there are side-channel analyses such as differential power analysis (DPA) or differential electromagnetic analysis (DEMA) which help to extract the secret keys from an insecure processor or FPGA [18]. Following are key technologies to improve IoT security:

Security side channel attack: Another threat is possible which are side channel attack rather than encryption and authentication. Such attack is more protected about how the information is presented rather than how the information is being transferred.

Interface protection: Many of the hardware devices and software designer's access by an application programming interface (APIs). To secure the interface it requires the ability to give the authentication only to the authorized devices and authorize person to exchange the information over network via using encryption so communication between secure channel.

Threat prediction and security analytics: We must also predict the future threats rather not only to monitor or control it. Whereas prediction of new threats leads to the new algorithm formation and new application of artificial intelligence to access the non-traditional attack strategies.

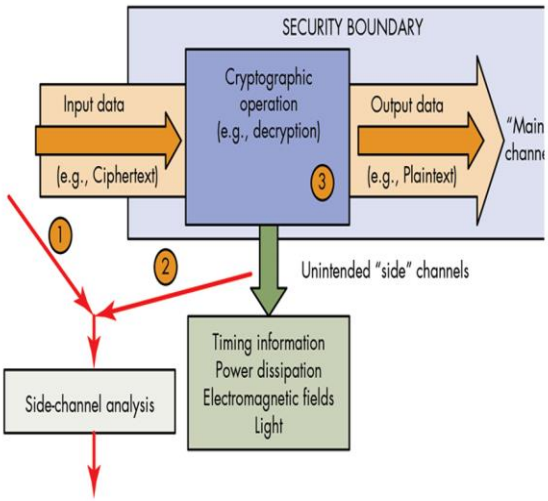

Fig. 6: Security Technologies of Attack

3. Application

1. Mobile networks [27, 28]

It provides a unique avenue for the detection of Sybil attackers as we observe the location of different devices and limits of realistic mobility that can be a constrain attackers. The identities of Sybil attacker always appear to move together but the defenses are not applicable beyond the mobile network.

2. Reputation System

It includes the many peer-to-peer system which have the AD-hoc networks and the online markets for the mitigation of the effects of malicious peers. The author Cheng and Friedman [29] says that the vulnerability of reputation system of SYBIL attack is being classified by symmetric or asymmetric approaches.

4. Proposed Work

In this paper, we proposed to use the trusted devices which help us to defend the SYBIL attack to the devices and make secure the data or information of our and they related to the trusted certification authority which is linked to the application and hardware devices. We proposed the CAM method where the comparing and matching is being done between the location IDs in the network traffic. CAM method is a process where the comparing is being done between the location IDS and the information of the nodes where the data is being send. While when we use the CAM method we can reduce the time and cost effective and more over the network size. We can perform this attack on the emulator COOJA for the accuracy.

N nodes is consisted by the WSN, consider a set G= {N0, N1, N2, N3, Ni}, where ni is the discrete sensor node in the network (G). Each node has a sensing region (R), which can intelligence the data in network within the region. Whereas, the system mode has four levels, first: initiation phase where each node should be recorded in the base station with location and their ID, and recorded data is placed in (r) table in base station by sending "Hello Packet" to base station. Second: in this network nodes are confidential and placed in the different sub-regions because of the network size is increasing. While the communication node communicates from one to another in the intra-region as well as

inter-region. Third: when a node requests a data from one region to another node in other region, a request take place when communication sense a Sybil node and it placed near to the node which requested. The nearest node will use the request node information such as location, node-ID and stab to collect information from another node and starts acting as a SYBIL node. The Sybil attack can be perceived by smearing the CAM (comparing and matching) method in the network.

The pseudo code for CAM is given below.

1. G-> N (nodes)
2. N nodes are movable and linked
3. Single node as a head node
4. K = {k1, k2, k3, k4, ……ki, kj…, kn} // assign region via head node
5. While [Ki associate with Kj]
6. If [key (Node i) == key (Node j)]
7. Data (Node i) → (Node j)
8. Pi ← position Є X, Y as source nodes
9. Pj ← position Є X, Y as destination nodes
10. If ((vj (xj, yj) == P j) and (vi (xi, yi) == Pi)) then
11. Vi refers data to vj
12. Else display ("Sybil node")
13. End if
14. End procedure

Defense Mechanism Against Sybil Attack

Sybil defense mechanisms are mostly decentralized solution, which means these designs operate without any centralized authority. It has two common assumptions: trust and algorithmic property (fast mixing property).

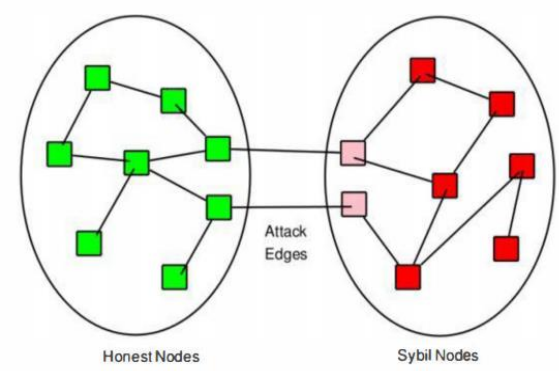

Fig. 7: Network with Sybil node and Honest node

Table 1: Defense mechanism of Sybil Attack

System name	Technique used	Merits	Demerits
Sybil guard	Random walk	It offers dramatically improved and optimal guarantees	It detects only Sybil node at a time
Sybil limit	Random walk	Improves the reliability	Work on fast mixing network (algorithmic property)
SyMon	Selected dynamically	Fast mixing property	Not appropriate for large network
Sybil defender	Partial random walk by node	Scalable and efficient	Failure cases
Sybil infer	Bayesian inference on result of random walk	Reliable than Sybil guard	Not scalable and computational overhead
Sybil shield	Resource testing scheme	Reduce false positive rate	Nodes increase falsely and also increase detected node level

General Approaches for Countermeasure Against Sybil Attack

There are few countermeasures developed against Sybil attack, many researches tried to build the new solution each time starting to get the overcomes of the previous solution disadvantage. There are various schemes has been developed to counter measure the Sybil attack are as follows. Firstly, Trusted Certification which is the first solution developed against the Sybil attack which tells that the centralized authority is being used to validate the entities and each entity is uniquely identified by the unique digital signature assigned by CA. This approach has the larger overheads when it applied to larger scale system also it is not cost efficient. Secondly, RSSI based Scheme which has a Sybil attack problem for the lightweight received signal strength schemes. In this scheme detector node is used to receive the RSSI value and identity of each node and to make it successful an additional node is required but it is unreliable.

Thirdly, Resource Testing has a main point of resource testing is the number of identities possesses fewer resources than it would be expected if they are independent. In this approach, a verifier calculates the resources such as energy, storage, capacity of identities. If node contains larger resources then a ravenous node is found and it would be considered as an attacker node. The verifier message may flood the network it considered as an unsuccessful scheme whereas to overcome this "radio resource testing" scheme is proposed where each node has a radio and it can transmit or receive radio signals only at one channel. Fourthly, Incentive based scheme based on the reward schemes where the economic incentives are used with a range of application area. This offers a reward to adversaries if the identity controllers are revealed and the target peer name is state by an identity when payment in exchange is received by it.

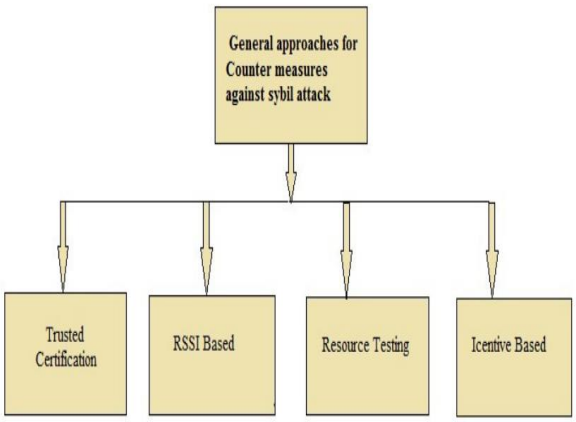

Fig. 8: General Approaches for Counter measures against Sybil Attack

Table 2: Countermeasures against Sybil Attack

	Trusted certification [34]	Resource testing [32]	RSSI based [33]	Incentive based [37]
Methodology	Centralized certification authority	Resources calculation	Radio signal strength	On rewards
Advantage network	Large overhead efficient	No bandwidth positive rate	False needed, robust	No clock synchro-nization
Disadvantage efficient	Less cost	Not complete defense	Less reliability	Inspire attackers economically
Application domain	General	General	Wireless sensor network	Ad-hoc network

5. Conclusion and Future Work

In this paper, we outlined the introduction of interne of things and the architecture of IoT where we have make a consideration in the network layer of IoT architecture the security issues, attack in the network layer and security challenges. There is the defense mechanism for the Sybil attack. The main and harmful attack in network layer is SYBIL attack. We have proposed the general approaches for the Sybil attack for the prevention and also a CAM method for the prevention of SYBIL attack in the network layer by comparing and matching the location IDs and the network size in data traffic. The future work would be that we can involve the improvement of the efficient detection mechanisms and cost effective in the network for specific detection rate to be optimized such as false positive and negative rate. We can also modify the CAM method reduces the time, cost and the network size. Whereas the throughput of the network should be higher rather than other security methods.

References

[1] F. Xia, L. Yang, L. Wang and A. Vinel, “Internet of Things,” International Journal of Communication Systems, John Wiley & Sons, Inc., pp. 1101-1102, 2012.

[2] Special section on testing and security of Web systems Alessandro Marchetto. Published online: 14 October 2008 © Springer Verlag 2008.

[3] J. Gubbia, R. Buyya, S. Marusic and M. Palaniswami “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems 29 (2013), pp. 1645–1660, Elsevier, 2013.

[4] K. Ashton, That “Internet of Things” thing, RFID Journal, 2009.

[5] A. Dunkels. The Contiki operating system (webpage). http://www.sics.se/~adam/Contiki/; accessed January 22, 2006.

[6] A. Dunkels, ‘Contiki: Bringing IP to Sensor Networks’, ERCIM News, no. 76, pp.59–60, Jan- 2009.

[7] L. Wang and A. Vinel, “Internet of Things,” International Journal of Communication Systems, John Wiley & Sons, Inc., pp. 1101-1102, 2012.

[8] A. Vinel, “Internet of Things,” International Journal of Communication Systems, John Wiley & Sons, Inc., pp. 1101-1102, 2012.

[9] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nano systems, in: co-operation with the working group RFID of the ETP EPOSS. Internet of Things in 2020, roadmap for the future, version 1.1, 27 May 2008.

[10] Xu Xiaohui „“ Study on Security Problems and Key Technologies of The Internet of Things”, 2013, International Conference on Computational and Information Sciences.

[11] Yan L, Zhang Y, Yang L T. The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, 2008.

[12] Shao Xiwen “Study on Security Issue of Internet of Things based on RFID” 2012 Fourth International Conference on Computational and Information Sciences

[13] SHEN changxiang, ZHANG Huanguo and FENG Dengguo, “Literature Review of Information Security”, Science in China (Series E: Information Sciences), vol.37, no.2, 2007, pp.129-150.

[14] WU chuankun, “A Preliminary Investigation on the Security Architecture of the Internet of Things,” Bulletin of Chinese Academy of Sciences, vol 25, no. 4, 2010, pp 411-419.

[15] N. Gershenfeld, R. Krikorian, D. Cohen, The internet of things, Scientific American 291 (4) (2004) 76–81.

[16] Anne James and Joshua Cooper, “Database Architecture for the Internet of Things,” IETE Technical Review, vol.26, 2009, pp.311 -312.

[17] https://www.microsemi.com/products/fpga-soc/design-support/fpga-soc-design

[18] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, A. S.K. Pathan, "A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks”, 3rd International Conference onEco-friendly Computing and Communication Systems (ICECCS) 2014 IEEE.

[19] T. G. Dhanalakshmi, N. Bharathi, M. Monisha, "Safety concerns of Sybil attack in WSN International Conference on Science Engineering and Management Research (ICSEMR), 2014 IEEE.

[20] K. Saleem, M. S. Khalil, N. Fisal, A. A. Ahmed, " Efficient Random Key Based Encryption System for Data Packet Confidentiality in WSNs, “12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013.

[21] X. Zhenghong, C. Zhigang, "A Secure Routing Protocol with Intrusion Detection for Clustering Wireless Sensor Networks, “International Forum on Information Technology and Applications (IFITA), 2010 (Volume:1) IEEE.

[22] P. R. Vamsi, K. Kant, "A lightweight Sybil attack detection framework for Wireless Sensor Networks”, Seventh International Conference on Contemporary Computing (IC3), 2014. IEEE.

[23] Makhdoom, M. Afzal, I. Rashid, "A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks", National Software Engineering Conference (NSEC), 2014. IEEE.

[24] M. Li, Y. Xiong, X. Wu, X. Zhou, Y. Sun, S. Chen, X. Zhu, "A Regional Statistics Detection Scheme against Sybil Attacks in WSNs", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013. IEEE.

[25] Liang Xiao, Student Member, Larry J. Greenstein, Narayan B. Mandayam, and Wade Trapper,” Channel-Based Detection of Sybil Attacks in Wireless Networks,” IEEE Transactions on Information Forensics and Security, Vol. 4(3), Sep. 2009.

[26] S. Capkun, J.-P. Hubaux, and L. Buttyan. Mobility helps peer-to-peer security. IEEE Transactions on Mobile Computing, 5(1):43–51, Jan 2006

[27] C. Piro, C. Shields, and B. N. Levine. Detecting the Sybil Attack in Ad hoc Networks. In Proc. IEEE/ACM Intl Conf on Security and Privacy in Communication Networks (SecureComm), August 2006

[28] V. Palanisamy, P. Anndaurai. Curbing and Curing Sybil attack in Ad-hoc network. ICAC 2009 p. 1-5

[29] Haifeng Yu, Michal Kaminky, Phillip B. Gibbon, Abraham D. Flaxman, Sybil guard: defending against Sybil via social networks, IEEE/ACM transaction on networking, jube 2008 vol. 16. P.576-589

[30] Haifeng Yu, Michal Kaminky, Phillip B. Gibbon, Feng xiao, Sybil limit: near optimal via social networks defense attack, IEEE/ACM transaction on networking, jube 2010 vol 16. P 885 - 898.

[31] James newsome, Elaine shi, Dawn song, Adrian perrig the Sybil attack in sensor networks: analysis and defense.

[32] M. demirbas, y. song. An RSSI based scheme for Sybil attack detection in wireless sensor network. Proceeding of international of symposium world of wireless, mobile, multimedia networks (WoWMoM’06) 2006 p. 564-570

[33] J R Douceur the Sybil attack in proceeding for the first international workshop on P2P system (IPTPS’02) vol 2429 Cambridge ma USA: springer-2002 p. 251-260

[34] zhi yang, jilong xue, xiaoyong yang, xiao wang and yafei dai. voteTrust: leveraging friend invitation graph to defend against social network Sybil, IEEE transaction on dependable and secure computing 2015 p. 1-14

[35] wei wei, fengyuanxu, chiu c. tan, member, IEEE and qun li, senior member, IEEE. Sybil defender: a defense mechanism for Sybil attack in large social network. IEEE transaction on parallel and distributed syste Dec. 2013, vol 24 p.2492-2502

[36] A. Margolin, N. Boris, L.B. Neil. informant: detecting Sybil using incentives. Proceeding of financial cryptography 2007 springer p. 192-207

[37] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal,” W ireless sensor network survey,” Computer Networks, Vol. 52, pp.2292-2330, April 2008.

[38] Vishal Rathod 1, Mrudang Mehta," Security in Wireless Sensor Network: A survey," Ganpat University Journal of Engineering & Technology, Vol.1, Issue-1, Jan.-Jun.-2011.
[39] Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi," Secure hierarchical routing protocols in wireless sensor network; security survey analysis," International Journal of Computer Communications and Networks, Vol.2(1), February 2012.
[40] T. Padmapriya and V.Saminadan, "Handoff Decision for Multi-user Multiclass Traffic in MIMO-LTE-A Networks", 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016) – Elsevier - PROCEDIA OF COMPUTER SCIENCE, vol. 92, pp: 410-417, August 2016.
[41] S.V.Manikanthan and V.Rama"Optimal Performance Of Key Predistribution Protocol In Wireless Sensor Networks" International Innovative Research Journal of Engineering and Technology ,ISSN NO: 2456-1983,Vol-2,Issue –Special –March 2017.
[42] P Bala Gopal, K Hari Kishore, B.Praveen Kittu "An FPGA Implementation of On Chip UART Testing with BIST Techniques", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015