ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, Januaury 2014

Security for Green Communication in Heterogeneous Wireless Networks

Elamathi.N[1], Dr.S.Jayashri[2]

Assistant Professor, Dept. of I.T., Adhiparasakthi Engineering College, Melmaruvathur, Tamilndau, India[1]

Director, Adhiparasakthi Engineering College, Melmaruvathur, Tamilndau, India[2]

ABSTRACT— The wireless network access is incredible growth in current and next generation mobile communication culture. By default in future generation, the wireless mobile node user's ratio must be increased. The security and energy consumption crisis in the wireless networks has become important role. The significant essentials of wireless networks are, to extend the efficient energy utilization, security of the network and network lifetime. In the heterogeneous wireless networks, the energy efficiency of wireless systems has to be significantly improved by green wireless communications. All communication technologies using several security methods for protecting network resources as well as data part also. Such types of schemes are having some issues .This paper, concentrated on security aspects of the heterogeneous wireless networks such as harmful network DDos attacks and secure solutions for those attacks. This survey paper mainly focused DDos attack that is mainly disturb the network life time, energy efficiency, delay. Many security schemes and distributed defense systems are availed. Such kind of attacks and secure solutions are over viewed here.

Keywords : Heterogeneous networks, next generation, energy efficient, green communications, DDos attack.

I. INTRODUCTION

In next generation wireless technology, the wireless network subscriber statistics are unimaginable. In the heterogeneous wireless networks, each wireless networks has own behavior and unique application, as made comparison with other networks. The tremendous growth of heterogeneous wireless network access, such kind of mobile subscribers growth is incur high data rate usage, more energy utilization of the nature. Now we are in the need on environmental conscious to reduce the energy consumption of our heterogeneous next generation networks.

The heterogeneous next generation wireless networks are fully engaged with high speed Internet access every place and every time. iPhone and other types of smart phones creates new traffic demand applications, such as mobile video, gaming, M-commerce. Such application causes unlimited data traffic. It requires more resource utilization and increasing energy consumption in the network. By default, the more energy consumption leads to the greenhouse gas emission. This is also a major threat for sustainability and environmental protection.

The Information technology and communication networks are also a partner in global warming causes, to increasing by the range of 2% green house gas emissions [1]. In wireless communication networks, all the mobile nodes and sensor devices has limited power capabilities. Within a time stamp the reliable communication must be performed in the network, if the communication is not completed within the allocated time stamp, automatically they required more energy from the network resources and reduce the power capabilities of the nodes in the network. Due this problem, the wireless network can get service interruption. Security is given much prominence in resources and network around the world. Security attacks can cause harmful service disruption in heterogeneous wireless 4G network. Such security threats may cause the performance degradation of network. On that time the utilization of the resource, and delay should be increased. Consequently the resource consumes more power for maintaining their energy. [2].

A secure communications has more robust and flexible security mechanism which is needed in mobile devices of heterogeneous networks, particularly mobile phones, portable communications services (PCS), and all the mobility devices in a network. This security mechanism provides unbreakable security for network mobility resources. It is a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, Januaury 2014

lightweight, reconfigurable security mechanism, and capable of capturing the dynamic behavior of mobility nature network. [3].

This paper is divided into sections organized as follows: Section 2 is a summary of the related work that consists of introduction to Heterogeneous wireless networks (hetnet), cryptography in hetnet, attacks and security frameworks. Section 3 describes the DDos security attack, security schemes for DDos attack. We conclude section 5.

II. RELATED WORK

i) Introduction To Heterogeneous Wireless Network

The next-generation wireless network architectures are dynamic and its infrastructure is expandable in nature. The entire Keys among these are increased diversity, not only in protocols and technology, but in the QOS parameters. This integrated communication provided by heterogeneous networks. A heterogeneous network (HETNET) is a network used to connect resources with different protocols and operating systems. The heterogeneous network is used in different technologies of wireless networks. For example, a wireless network which provides a service through a WIMAX and is able to maintain the service when switching to a LTE is called a wireless heterogeneous network. [4]. The wireless communication provides better performance characteristics of network in terms of mobility, flexibility but in security aspect, it spends more expense because of its open communications. Automatically it raises the security vulnerabilities with some additional security threats in the heterogeneous wireless networks. [3]

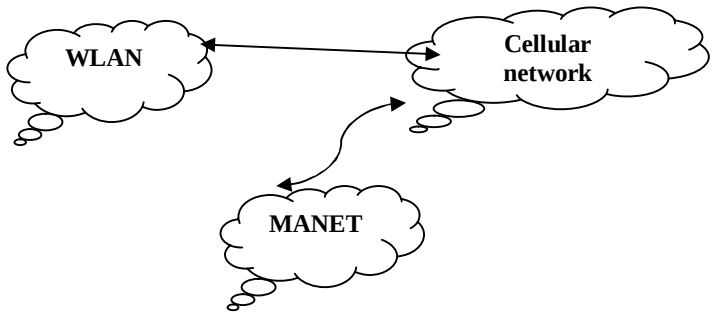

Fig.1.Heterogeneous wireless network

ii) Cryptography In Heterogeneous Wireless Network

The Security in heterogeneous wireless network has some different forms of facets such as authentication of resources in the network, authorization for the user, data confidentiality, pure Non repudiation, better availability and integrity constraints. Authentication provides each and every user or resources in the network, to validate each other's authentic identity. Authorization majorly referred to as access control, which provides the ability to determine whether a user should have the permission to access specified networks, or not. Integrity provides the protection to the information from the unauthorized user.

Confidentiality referred as privacy, it keeps the information in secret. Only the authorized person can understand that information .In Availability, the network operators should prevent outside malicious users from blocking legitimate access to a network or a network service. Denial-of-service, for example, will deter legitimate users from accessing the network information and resources. Non-repudiation refers to the ability for a network to supply undeniable evidence to prove the message transmission and network access performed by a user. [5]

iii) Attacks In Heterogeneous Wireless Networks

In heterogeneous networks, some of the common active attacks are interrupt the normal flow and speed of communication. This disruption causes the transmission delay in the network. It requires more utilization time,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, Januaury 2014

excessive amount of energy for the network. A Denial-of-service (DoS) attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to it users. For example, an attacker may initiate a large number of connections to a target destination continuously to overload the target to make it impossible or difficult for the target to provide any service. The DDos attack is multiple hosts attack to the nodes in the network simultaneously.

Masquerade: An attacker first acquires the identity of a authenticate user. It then pretends to be an authorized user to access the network information and resources.

Man-in-the-middle: An attacker forces between source and destination to intercept and manipulate the messages transmitted among the transmission path.

Replay Attack: An attacker observes and records the legitimate transmission. The attacker then resends the messages later on. Using replay attacks, an attacker could pretend to be an authorized user to access a network or information even when the captured transmission was encrypted and even when the attacker does not know the security key needed to decrypt the captured transmission. To overcome these attacks rigid security protocols and algorithms are defined. But till now such types of secure algorithms and protocols has some deficiency.

iv) Security Algorithms And Distributed Defense System

The secure encryption/decryption algorithms can be categorized into two types: secret-key algorithms and public-key algorithms. Conventional encryption techniques employ secret-key algorithms. Using a secret-key algorithm, the communicating parties share the same secret key. The main disadvantages of the secret key algorithm is that the 2 parties sending messages to each other must agree to use the same private key before they start transmitting secure information. This may be impossible because the two nodes who want to communicate with each other through a secure routing means, that they will need a secure way to tell each other what the private key will be, if there were a secure way to do this, and then the cryptography would not have been necessary in the first place in order to create that secure channel.

If the secure secret keys can be transmitted over the network, it also implies that other data should also be transmitted securely over the network. Different keys are used in public a key algorithm, which is also referred as asymmetric algorithm. Each user should have both public key and private key. Compared with secret key algorithms, the public key algorithms are efficient one for providing tight security to network. But there are also some limitations to achieve unbreakable security solutions over the routing as well as data or message part also in the network.

Asymmetric key cryptography is not feasible for bulk messages. It takes long time to do encryption and decryption process in the network. But in some network environment the symmetric key cryptography is very useful and may be some other cases the asymmetric key cryptography is useful one.

III) DDos Attack

In the real time environment distributed denial of service attack is frequently collapse the network. Finally the heterogeneous wireless network is observed more energy and power for communication among the resources in the network. To overcome DDos attack in the network, many security algorithms or frameworks are defined and implemented. This paper mainly focused on few security methodologies for DDos attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, Januaury 2014

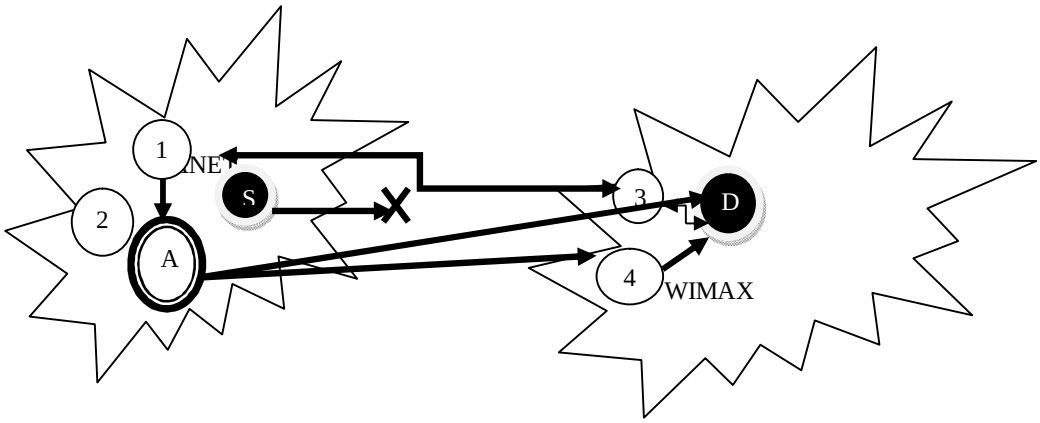

Figure.2
DDos Attack in heterogeneous wireless network

A---(Master node)ATTACKER, S----SOURCE NODE, D---DESTINATION NODE , 3,4---NORMAL NODE

Multiple coordinated attacks from multiple resources in the network cause DDos malicious attack. It will use millions of nodes in the network as malicious and sends unwanted messages from those nodes to the target node. On that time it makes heavy traffic in the network. In DDoS attack, the hacker makes use of susceptibility in one node and making it as DDoS master. This master node acts as the intruder, which recognizes and communicates with other nodes that can be compromised. It has more number of cracking tools.

An intruder uses the single command and instructs to other thousands of nodes to launch one of many flood attacks against a specified target. The stream of packets to the target node causes a denial of service. A node comes under the control of a master intruder is known as a zombie or bot and group of zombies are called as botnet or zombie army, which is identified as the biggest threat to Internet security. [6]

A) Survey Of Security Solutions For DDos Attack

Monitoring, analysis, and filtering of traffic are three major phases in solution against to the DDos attack. Each secure distributed defense mechanism has metrics called deployment, detection, security, and robustness of the network. [7]. The DDos attack process is similar to congestion-control problem .In DDos attack affected network, the intruders are create congestion. Those DDos intruders not obeying traditional congestion control mechanisms in the network. On that time the push back mechanism placed each router in the network, and it is used to detect and drop that flooded malicious packets [8].

There are also some disadvantages. The pushback mechanism cannot participate with contiguous deployment and it cannot detect and that messages are coming from intruders. To overcome this limitation, again the push back scheme refined .This enhanced version of pushback scheme called selective pushback (SPB).[9]. The SPB sends the messages to the routers, that is placed nearer to the attack sources. In this scheme, we analyze the traffic distribution in the network. Both processes are used to detect and locate the intruders. It is also used to diminish the attack damage more quickly. But still accuracy of detection and deployment across the heterogeneous wireless networks are remain big issues. If we identified the attack in the network, then first separate the malicious route from the legitimate route in the network (i.e.) isolate the malicious packet flows from the original packet flow. In the wireless network, each and every route should have a threshold byte value for sending to the target node. If the threshold byte value exceeds in any flow, that specified flow route consider as attacked routing. Because DDos attack create a master malicious node and its zombies.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, Januaury 2014

Now that zombies are sends packet tsunami to the target node. Due to this, the network needs more energy, more power consumption of resources, reduced its life time. Now we want to differentiate the normal state of the network flow and suspicious state of network flow using the parameters Upper control limit and lower control limit, which are used in the six sigma method. [10].The ANN technique is used for detects and differentiates the zombies from legitimate resource network. [10].Each distributed DDos defense system should have the key metric issues called robustness, deployment, security, detection, implementation and response. These metrics are analyzed in various distributed schemes. [7]. SOS is one of the distributed DDos Defense systems, which is used to verify the legitimate user and send the packets to the target node with help of some secret servlet, that tunnel it. Active Security System (ASSYST) is another defense system. It is designed and implemented for distributed response with non-contiguous deployment at edge networks. CROSSACK is used to filtering the attack routing in the heterogeneous wireless network

IV) Conclusion and Future Work

Heterogeneous wireless networks provide best quality of service to the users without affecting the natural parameters of the environment. This network provides, the best communication on different IP backbone based networks at anywhere and anytime. Security becomes the most challenging aspect or issue in Green heterogeneous wireless networks because of some network harmful attacks. This survey paper focused the security aspect of heterogeneous network. Main concentration of this survey paper is overview of harmful attack called Distributed denial of service attack and its different types of distributed defense security systems with advantages and disadvantages of those systems. Till now, the DDos attacked network requires more power consumption for their zombies, utilization of several resources in the network. In spite of this, the DDos attack causes poor transmission, delay, and minimum lifetime duration of the network. In Future work, these challenging issues are needed to be fully overcome. On that time the heterogeneous wireless networks provides secure green communication over different networks.

REFERENCES

[1]. JALAL AL-MUHTADI, DENNIS MICKUNAS, AND ROY CAMPBELL "A LIGHTWEIGHT RECONFIGURABLE SECURITY MECHANISM FOR 3G/4G MOBILE DEVICES",IEEE WIRELESS COMMUNICATION ISSN 1536-1284 2002, VOL. 9, PP. 60-65 (12 REF.) (2002) ,UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN.

[2]. "The impact of ICT on global emissions, on behalf of the Global eSustainability Initiative "(GeSI), McKinsey & Company, Tech. Rep.,Yongsuk Park, Taejoon Park (2007) IEEE Globecom Work-shop, 1-6.

[3].http://en.wikipedia.org/wiki/Heterogeneous_network"

[4]. Jyh Cheng chen ,tao zhang "IP based next generation networks, system , architectures, and protocols", Publisher: Wiley January2004 ISBN: 0-471-23526-1.

[5]. [Neumann 2000] P. G. Neumann, Denial-of-Service Attacks. Communications of the ACM 43, 4, 136. 2000.

[6]."A Comprehensive Survey of Distributed Defense Techniques against DDoS Attacks", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.12, December 2009

[7] John Ioannidis, ."Implementing Pushback:Router-Based Defense Against DDoS Attacks ",AT&T Labs Research. 03/2002-citeseer;

[8]. Peng, T., Leckie, C. and Ramamohana rao, K "Defending against distributed denial of service attack using selective pushback. ".(2002)". Proceedings of the 9th IEEE International Conference on Telecommunications (ICT). P.no 411-429. China.

[9]." An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based approaches", by B. B. Gupta, Manoj Misra and R. C. Joshi, Journal of Information Assurance and Security 2 (2008) pp102-110 1554-1010 © Dynamic Publishers, Inc .

[10] Brij Bhooshan Gupta , Ramesh Chand Joshi , and Manoj Misra."ANN Based Scheme to Predict Number of Zombies in a DDoS Attack",International Journal of Network Security, Vol.14, No.1,PP.36–45,Jan.2012.