ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 4, Issue 11, November 2017

Network Security in WSN Providing Selective Forwarding Algorithm

[1] Supriya.B.N, [2] Yeshashwini.S, [3] Shruthi.S.R, [4] Sushma.G.K

Abstract: - **It explains about how to secure computer networks, the network security mainly includes "cybercrime technology" and "hacking". Some hackers will damage the web server and replace their logo with pornography, they will hack e-mails, credit card number through online shopping sites. This paper addresses the ethical hackers: their skills, attitudes etc., The hacker should have the brilliant mind to hack anything, some rules he should follow to become an ethical hacker called as "penetrate testing". The rules consist the knowledge of HTML, javascript, computer tricks, breaking, cracking etc., WSN's having many types of attacks because it deployed in the open and unprotected environment. So that we are using one algorithm to detect the attack called as "selective forwarding attack" and it damaged attacks in multi-hop routing protocols. Detection algorithm based only on the neighbourhood details and it detects SFA's with high accuracy. Like this, we can detect attacks and provide security for the system. Network security is the main issue of computing because types of attacks are increasing day by day. The malicious nodes create a problem in the network. So we have to provide network security elements such as confidentiality, integrity and availability and these vectors.**

Key Words- **Cybercrime, Hacking, Penetrate testing, Security, Wireless sensor network.**

I. INTRODUCTION

Computer Networks Security (CNS) is becoming more important nowadays because of increasing demand for internet based technologies. The increase in users privacy concerns is related to the increasing use of the internet[1] . However, security mechanisms that prevent such issues might deteriorate a user experience. A user might find these mechanisms cumbersome or unnecessary and neglect using them, which might lead to security breaches in certain systems or simply loss of privacy of the user. In the growth of the technology many hackers argue that they follow an ethic that guides their behavior and justifies their break-ins.

Wireless mesh network (WMN) is a communication network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may, but need not, connect to the Internet. WMNs are emerging as a promising solution to provide high speed Internet access due to the advantages of scalability, self management and low up-front cost U.S. military forces are currently using WMNs to connect their computers in field operations. In network security there are some attacks such as selective forwarding attack, existing methodology, sinkhole, cyber crime technology.The term cyber terrorism is becoming increasingly common in the popular culture, yet a solid definition of the word seems hard to come by. While the phrase is loosely defined, there is a large amount of subjectivity in what exactly constitutes cyber terrorism. If you ask 10 people what 'cyber terrorism' is, you will get at least nine different answers! When those10 people are computer security experts, whose task it is to create various forms of protection against 'cyber terrorism', this discrepancy moves from comedic to rather worrisome. When these 10 people represent varied factions of the governmental agencies tasked with protecting our national infrastructure and assets, it becomes a critical issue.

II. BACKGROUND

2.1 Security Goals

When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services:

• Confidentiality: Confidentiality aspect refers to limiting the disclosure and access of information to only the people who are authorized and preventing those not authorized from accessing it.

• Integrity: Integrity measures the data in a consistent, accurate and trust worthy manner over the period in which it will be existent. it ensure that un authorized people do not alter the data.

- Authentication: Authentication enables a node to ensure the identity of the peer with which it is communicating.
- Availability: availability refers to the up time maintenance of all resources and hardware. It can also involve carrying out of regular hardware repairs.

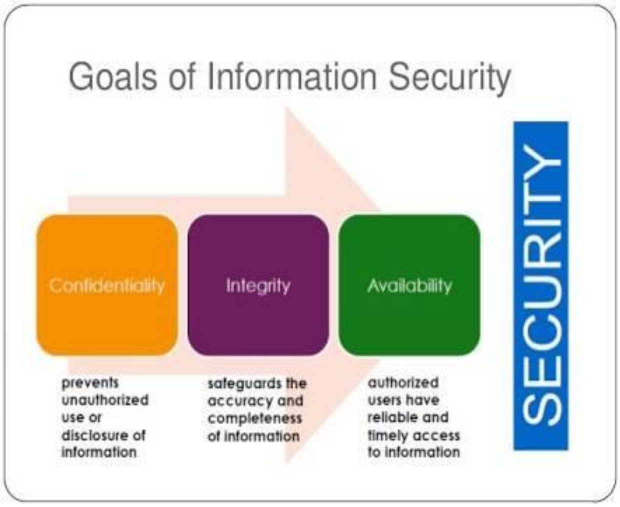
Goals of Information Security
Confidentiality
Integrity
Availability
SECURITY
prevents unauthorized use or disclosure of information
safeguards the accuracy and completeness of information
authorized users have reliable and timely access to information

Fig-1: Demonstration of security goals

2.2. Security Challenges

We summarize security challenges in sensor networks as follows:

- Malware with worm capabilities.
- Release of more shadow brokers tools.
- Getting back to basics (patching, endpoint, hyglene).
- Adapting the firewall to face new threats.
- Monitoring cloud configuration and security.

III. RELATED WORK

3. 1 SELECTIVE FORWARDING ATTACK

In this type of attack the attacker may not forward a packet. A multi-hop acknowledgements scheme to launch alarms is proposed in [2]. Each node in the forwarding path is in charge of detecting malicious nodes. If an any node detects a node as malicious then it will send an alarm packet to the through multi hops. Mainly consists of two streams namely downstream and upstream .Downstream detection denotes on base station and upstream detection denotes towards source node[3]. To sends the packet from source to the destination the intermediate nodes choose a correct path and sends packet without making any delay. In [4] the HSN consists of powerful high-end sensors (H-sensors) and large number of low-end sensors (L-sensors). After deploying sensors, a cluster formation takes place with H-sensor as cluster head. Whenever packet drops occur at a node, L-sensor nodes report the packet drop to a cluster head (an H-sensor). Based on the reports received, H-sensor runs a test and determines whether a node I is ready to accept or not. For each node, probability value ‟p‟ is calculated which is equal to the percentage of dropped packets in all forwarded packets. This division takes place at proper time. The condition is that every topology has to completely the work within the given time. If the network is divided into four topologies and suppose an event is raised, nodes in both the topologies sense the event, raises an event packet and forwards to the base station. Suppose a malicious node drops packet in one topology, still packet reaches base station through path in another topology. By using their location information base station can detect malicious node.

3.2 SINKHOLE ATTACK

Sinkhole attack is an inside attack were node inside the network and creates an attack. Then the attacked nodes try to try to access all the nodes based on some routing protocols. Due to communication between the nodes of wireless sensor network of many to one communication . where each node send data to base station. Sinkhole Attack in Protocol This is another explanation of sinkhole attack in wireless sensor network and this time the attack is launched under Tiny AODV (Ad-hoc On Demand Vector) protocol. Tiny AODV protocol is the same as AODV in MANET but this one is lighter compared to AODV and it was modified purposely for wireless sensor network [5]. The sinkhole node or compromised node launches an attack by send back RREP packet. In RREP packet it gives small number of hops which indicates close proximity to the base station. Then the source node decides to forward packet to sinkhole node.

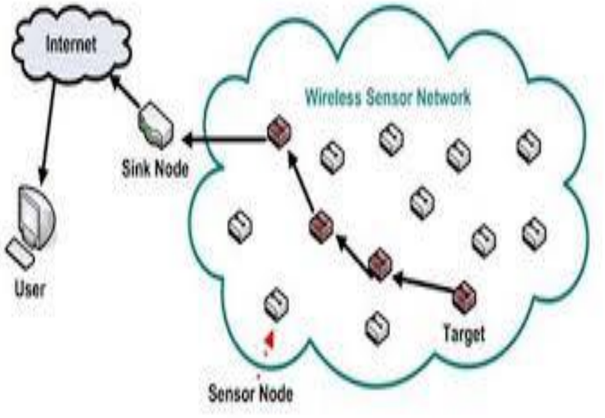

Fig-2: Sinkhole attack

3.3 EXISTING METHODOLOGY

The control system security efforts address two predominant issues: a) how to secure older, proprietary networks, and b) how to secure new system. Attack Methodology Analysis

(AMA), can be used to validate exploit technology that can be used against control system environments, identify gaps that exist in control system defenses, and associate known mitigation techniques with the defensive gaps. This research maps IT-based exploit tools and attack methodologies to specific vendor Control systems, thereby supplying defend with pertinent information regarding the detection and mitigation of cyber threats to control systems, and also by using "Random Password Generator" RPC generates the random passwords so hackers can't hack the data.

Fig-3: Existing methodology using RPC

3.4 CYBER CRIME TECHNOLOGY

Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact[6].

Following on from the discussions above, it becomes obvious that the most likely 'weapon' of the cyber terrorist is the computer. Thus, one might ask, are we arguing that one should restrict access to computers, just as access to explosives is restricted? Not quite, but close. We believe that the stockpile of connected computers needs to be protected. There are many laws that define how one should protect a firearm from illegal/dangerous use. The mandatory use of trigger locks, though controversial, has been put forward to prevent danger[7].

Fig-4:Cyber Crime Technology

IV. TYPES OF HACKER

4.1 SCRIPT KIDDIE:

Script kiddies normally don't care about hacking.They just copy and use it for a virus. A common script kiddle attack is Dosing or DDosing in which they flood an ip with so much inform it collapse under the strain.

4.2 WHITE HAT HACKER:

Also referred as Ethical Hacker or sometimes called as Sneakers. They will help you remove a virus company. They are with good courage to fights against Black Hat.

4.3 GREEN HAT HACKER:

It identified as "n00bz" but unlike script kiddies. They often flamed by the hackers community for asking many questions.

4.4 GREY HAT HACKER:

They are Skilled Hacker who use his skills for legal or illegal acts but not for personal gains. Grey Hacker present in between White Hat and Black Hat hacker

4.5 WHITE HAT HACKER:

Also referred as Ethical Hacker or sometimes called as Sneakers[8]. A White Hat Hacker mainly focuses on securing corporate Network from outsider threat. They are with good intention that fights against Black Hat.

4.6 BLACK HAT HACKER:

Also referred as cracker A Black Hat Hacker's intention is to break into others Network, and wish to secure his own machine. They often use different techniques for breaking into systems which can involve advanced programming skills and social engineering.

V. HACKING METHODS

5.1 Bait and switch

Using this technique, the hacker runs a malicious program which the user believes to be authentic .after installing malicious program on your computer, the hacker gets unprivileged access to your computer.

5.2 Cookie theft

The cookies of a browser keep our personal data such as a browsing history, username, and password for different sites that we access.

5.3 Click jacking attacks

Click jacking is also known by a different name, UI redress. In this attack, the hacker hides the actual UI where the victim is supposed to click.

5.4 Phishing

Phishing is a hacking technique using which a hacker replicates the most accessed sites and traps the victim by sending that spoofed link.

5.5 Virus, Trojan etc.

Virus or Trojans are malicious software programs which get installed into the victims system and keeps sending the victims data to the hacker.

VI. PREVENTION

Check the URL when login into any social networks and else to prevent from such attacks it is sufficient if we just see the source code and find the word “action” and see the task related to it.

6.1EMAILSPOOFING

This represents the act of fake emails that we receive in our mail box saying that they are from some higher authority and ask for your user name and password. this can also be associated to phishing.

6.2 BRUTE FORCE ATTACKS

A brute force attack consists of trying every possible code, combination, or password until you find the right one. The hacker tries out different combinations of dictionary to match the username and password.

- Is there a mechanism which will lock the attacker out after a number of failed attempts? Increasing Security against a Brute Force Attack from the example above, account security could be increased by:
- Increasingthe length of the password.
- Allowing the password to contain characters other than numbers, such as *or #
- Imposing a 30 second delay between failed authentication attempts.
- Locking the account after 5 failed authentication attempts.

6.3KEYLOGGING

Keystroke logging (often called key logging) is a method of capturing and recording user keystrokes. The technique and name came from before the era of the graphical user interface; loggers nowadays would expect to capture mouse operations and screen shots. A hacker when has access to the victim’s system installs a key logger or if he has no access he makes the user believe the key logger is some trusted application and makes him install it .It records all the users‟ activities (which also include usernames and passwords) in a local file called log file. The hacker somehow receives the log file and hence the victims system is hacked.

6.4 KEY LOGGER

Based on the order of the keystrokes, it is usually easy to identify the password(s) from the file later. Like the Trojan, this also requires that someone actually type the password. Key loggers come in two types: hardware and software . A hardware key logger can be fitted between the keyboard cable and the computer and can be activated with a few keystrokes. It is then left in place until after the password that you are looking to recover is typed. Later it is removed and the file of keystrokes is examined for the password. A hardware key logger is indictable by anti-virus software. A software key logger is installed on a system and effectively has the same function, however, it is a little bit more complex to use since it must be installed to run stealthily to be effective. A key logger could be used to steal a password from someone who is using an office computer or sharing a computer.

6.5 Using Two-Hop Neighbour Knowledge to detect Selective forwarding Attacks in wireless sensor.

The authors have used two- hop neighbour knowledge as a part of their attack detection process to ensure that the neighbour node to which the current node forwards the relaying packet is actually the neighbour of the current node and lies on the right path to the sink. The scheme is distributed in nature which means the sensor nodes collaborate to detect the presence of the attack. Each sensor node in the network is equipped with the detection module built on the application layer and is responsible to passively detect the selective forwarding attack in its neighbour node. This detection scheme, like many other existing schemes, takes advantage of the broadcast nature of the sensor networks. The nodes within the intersection of radio ranges of the source and the destination monitor their neighbourhood and raise alerts when the attack is detected. The authors have used the over-hearing mechanism for MAC (medium access control) layer to reduce the number of redundant alert packets sent to the base station[9].

VII. CONCLUSION

programmer even more than a normal programmer. Everyone in this paper, a survey is given on existing attacks in wireless networks. We have also covered the Random password generator , trigger locks, Two-Hop neighbour knowledge and protocols against those attacks, and mentioned some open research issues. This paper helps the readers to have better view of attacks and countermeasures in networks, and find their way to start secure designs for these networks. And also Hacking is now an issue that does not have any conclusion. The only way we can stop a hacker is by learning hacking. By learning we can read the minds of a hacker which enables us to know the reality. Hacking is not a crime but it is made a crime by misusing the knowledge of programming. Every hacker is a perfect should know the ethics of hacking and follow them to be safer.

REFERENCES

[1] A. Anton, J. Earp, and J. Young. How internet users‟ privacy concernshave evolved since 2002. Security Privacy, IEEE, 8(1):21 –27, Jan-Feb2010.

[2] Bo Yu, and Bin Xiao, “Detecting Selective Forwarding Attacks in Wireless Sensor Networks", Proc. 20th International Parallel and Distributed Processing Symposium IPDPS 2006 (SSN2006), Page(s):1 – 8, Greece, 25- 29April 2006

[3] Tran Hoang Hai and Euinam Huh “Detecting selective forwarding attacks in wireless sensor networks using two-hop neighbor knowledge” In NCA, pages 325– 331, 2008.

[4] Jeremy Brown and Xiaojiang Du “Detection of selective forwarding attacks in heterogeneous sensor networks”
In ICC, pages 1583–1587, 2008.

[5] Teng, L., and Zhang, Y. (2010). Secure Routing Algorithm against Sinkhole attack for Mobile Wireless Sensor Network, In Computer Modeling and Simulation, 2010. ICCMS’10. Second International Conference on (Vol. 4 pp.79-82). IEEE..

[6] DOC, 2002. US Department of Commerce, Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774. Sections 740.13, 740.17 and 742.15 are the principal references for the export of
encryption items.

[7] DOD, 2002. Department of Defense Education Activity Internal Physical Security. Department of Defense. DoDEA Regulation 4700.2

[8] A Study Of Network Security Using Penetration Testing by R. Shanmugapriya.

[9] Tran Hoang Hai and Eui-Nam Huh, Detecting Selective Forwarding Attack in Wireless Sensor Networks using Two-Hops Neighbour Knowledge, 7th IEEE International Symposium on Network Computing and Applications, 2008, 325-331.