Volume 4, Issue 2, April 2017 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Link Isolate for Trust Based Suspect ON-OFF Attack

Manisha Shrivastava
Research Scholar M.Tech. (Cyber Security)
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email: mani.shrivastava.lbs@gmail.com

Abhishek Pandey
Assistant Professor
Department of Computer Science & Engineering
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email: abhishekpandey@takshshila.org

ABSTRACT

A trust management scheme can be used to aid an automated decision-making process for an access control policy. Since unintentional temporary errors are possible, the trust management solution must provide a redemption scheme to allow nodes to recover trust policy. However, if a malicious node tries to disguise its malicious behaviors as unintentional temporary errors, the malicious node may be given more opportunities to attack the system by disturbing the redemption scheme. Existing trust management schemes that employ redemption schemes fail to discriminate between temporary errors and disguised malicious behaviors in which the attacker cleverly behaves well and badly alternatively. So in my dissertation work we present the vulnerabilities of existing redemption schemes, and describe a new trust management and redemption scheme that can discriminate between temporary errors and disguised malicious behaviors with a flexible design. We show the analytical results of the trust management scheme, and demonstrate the advantages of the proposed scheme with simulation conducted in a Wireless Sensor Network. We are make a Trust management system for the WSN with the new redemption scheme that able to optimize the existing temporary error and malicious node behaviors in the way of cyber security area.

Keywords:— *WSN, Malicious node, on–off attack.*

I. INTRODUCTION

Trust Management System

Trust is an important but complex concept in social science. Trust helps people to make decisions in unpredictable circumstances by reducing the uncertainty. Many distributed systems can be unpredictable and uncertain when the entities try to collaborate with each other. Because of the great number of possible threats in the varying applications that can be deployed through a distributed system, applying trust in such systems can be quite complex. Research on trust management [1] schemes, which manage trust and decide policies, has emerged as a challenging issue. Trust management schemes aim to improve collaboration between the entities in a distributed system by predicting future behaviors of peers based on their previous behaviors. A trust management scheme typically does this using the following steps. First, each node observes and stores the neighboring nodes' behaviors. Second, each node collects and stores the warnings or reports from other nodes about its neighboring nodes. Third, each node calculates the trust based on the behavior information collected and stored for each neighboring node. Last, based on the trust and the policies that use the trust, each node decides the best node or group of nodes

with which to collaborate. In some systems, trust management schemes allow trust redemption in order to allow a node to regain the trust of its neighbors. For instance, a Wireless Sensor Network (WSN)[2] is composed of sensor devices that have constrained resources and unreliable radio for wireless communication. Thus, there exists a possibility that unintentional temporary errors might occur. When a node performs a bad behavior (BB) [3][4][5], like a dropped packet, it could be considered malicious even if the behavior was temporary and unintentional.

Various Type of TSM-

CORE DESIGN ISSUES OF TRUST ESTABLISHMENT METHODS Trust can be established in a centralized or distributed manner as shown I the figure

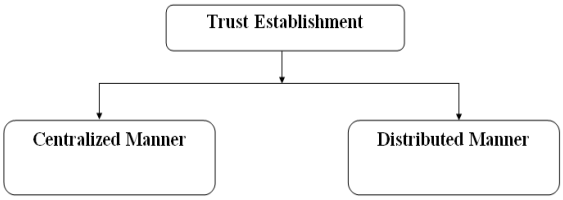

Figure 1.1 Trust Establishment

Obviously, MANET and sensor networks widely used for distributed trust management, where each network entity maintains a trust manager. The basic elements of such a trust manager is illustrated in Figure 1.1.

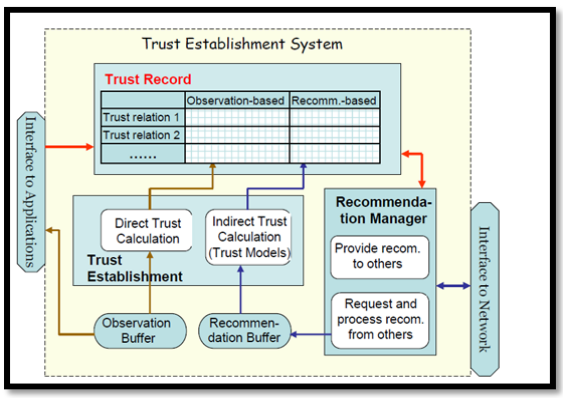

Figure 1.2 Trust Management System

Trust Record Stores–

Information about trust relationship and associated trust values. A trust relationship[7] is always established between two parties for a specific action. That is, one party trusts the other party to perform an action. In this work, the first party is referred to as the subject and the second party as the agent. A notation subject :agent; action is introduced to represent a trust relationship. For each trust relationship, one or multiple numerical values, referred to as trust values, describe the level of trustworthiness. There are two common ways to establish trust in computer networks. First, when the subject can directly observe the agent's behavior, direct trust can be established. Second, when the subject receives recommendations from other entities about the agent, indirect trust can be established. Direct Trust is established upon observations on whether the previous interactions between the subject and the agent are successful.

1.4 Cyber Security-

Cyber security[8] involves protecting information and systems from major cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage. In their most disruptive form, cyber threats take aim at secret, political, military, or infrastructural assets of a nation, or its people. Cyber security is therefore a critical part of any governments' security strategy. The U.S. federal government for example, has allotted over $13 billion annually to cyber security since late 2010. Table 2.1 show the list of Cyber Attack with its Description.

With cyber threats in a state of rapid and continuous evolution, keeping pace in cyber security strategy and operations is a major challenge to governments. Cyber security is a serious concern to private enterprise as well, given the threat to intellectual property and privately-held critical infrastructure. Advisory organizations such as The National Institute of Standards and Technology (NIST) and the

International Organization for Standardization (ISO) have recently updated guidelines to promote a more proactive and adaptive approach that prescribes continuous monitoring and real-time assessments.

Table 1.1 Cyber Attack list[9]

S.No	Type of Cyber Attack	Cyber Attack Description
1	Cyber Terrorism	Cyber terrorism is the disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes the form of attacks on networks, computer systems, and telecommunication infrastructures. For example, in response to the removal of a Russian WWII memorial in 2007, Estonia was hit with a massive distributed denial of service (DDoS) attack that knocked almost all ministry networks and two major bank networks offline. The rise in such cyber terrorism attacks is measureable: in the U.S., head of Military Cyber Command Keith B. Alexander stated that cyber attacks on facilities classified as critical infrastructure in the United States have increased 17-fold since 2009.
2	Cyber Warfare	Cyber warfare involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption. In the US and many other nation-states, cyber warfare has been acknowledged as the fifth domain of warfare (following land, sea, air, and space). Cyber warfare attacks are primarily executed by hackers who are well trained in exploiting the intricacies of computer networks and operate under the auspices and support of the nation-states. Rather than "shutting down" a target's key networks, a cyber warfare attack may intrude networks for the purpose of compromising valuable data, degrading communications, impairing infrastructural services such as transportation and medical services, or interrupting commerce
3	Cyber Espionage	Cyber espionage is the practice of using information technology to obtain secret information without permission from its owners or holders. Cyber espionage is most often used to gain strategic, economic, political, or military advantage. It is conducted through the use of cracking techniques and malware. In the US, the Office of the National Counterintelligence Executive released a report in 2011 officially acknowledging the legitimate threat of cyber espionage and its potential to damage the United States' strategic economic advantage.

1.5 Introduction to Cyber Risks-

Cyber risks can be divided into three distinct areas:

Table 1.2 Cyber Risk[8]

S.No	Cyber Risk	Explanation
1	**Cyber crime**	Conducted by individuals working alone, or in organized groups, intent on extracting money, data or causing disruption, cyber crime can take many forms, including the acquisition of credit/debit card data and intellectual property, and impairing the operations of a website or service
2	**Cyber war**	A nation state conducting sabotage and espionage against another nation in order to cause disruption or to extract data. This could involve the use of Advanced Persistent Threats (APTs).
3	**Cyber terror**	An organization, working independently of a nation state, conducting terrorist activities through the medium of cyberspace.

Organizations that have to consider measures against cyber war or cyber terror include governments, those within the critical national infrastructure, and very high-profile institutions. It is unlikely that most organizations will face the threat of cyber war or cyber terror.

1.6 Type of Cyber Attack[12]-

Table 1.3 Cyber Attack[10][11]

S.No	Cyber Attack	Cyber Attack Description
1	**Backdoors**	Backdoor is a type of cyber threat in which the attacker uses a back door to install a key logging software, thereby allowing an illegal access to your system? This threat can turn out to be potentially serious as it allows for modification of the files, stealing information, installing unwanted software or even taking control of the entire computer.
2	**Denial-of-Service Attack –**	A denial-of-service or a DOS attack generally means attacking the network to bring it down completely with useless traffic by affecting the host device which is connected to the internet. A DOS attack targets websites or services which are hosted on the servers of banks and credit card payment gateways.
3	**Direct-access Attack –**	A direct-access attack simply means gaining physical access to the computer or its part and performing various functions or installing various types of devices to compromise security. The attacker can install software loaded with worms or download important data, using portable devices.
4	**Eavesdropping**	As the name suggests, eavesdropping means secretly listening to a conversation between the hosts on a network. There are various programs such as Carnivore and NarusInsight that can be used to eavesdrop.

1.7 Problem Definition

1.8 Existing System

Existing redemption schemes are vulnerable to an On-off attack, which is specifically designed to disrupt the trust management and redemption schemes. By behaving well and badly alternatively, the On-off attack aims to make the trust management scheme consider a bad behavior as a temporary error. Thus, the malicious node would remain active and would have more opportunities to attack the network. Moreover, there may be circumstances under which an On-off attacker should be allowed to remain in the system. That is, if the cost of removing the attacker is higher than the cost that the attack imposes on the system, then it may be better to leave it alone. The major limitation of this system is do not allow discrimination of On–off attack that means that some the node in the network domain is given the good result in terms of packet sending ration and sometimes same node behave badly and not given the good result and make a damage of data and packet during the travel in

WSN Network. In general, if the malicious node performs n good behaviors and m bad behaviors alternating, we refer to this as an nG-mB On-offattack. For example, 4G-1B attack node means the nodebehaves well four times and behaves badly one time alternatively. This can also be called a 80 percent G-20 percent BOn-off attack.

1.9 Proposed System

- To propose a method to control the On-off attack and allow a system designer to decide the amount of risk allowed by an On-off attack.
- To presents a trust management scheme that uses a new kind of trust, called Predictability Trust (PT), which is able to predict future trust values based on past behaviors with an efficient and flexible design.
- For each node to detect neighboring On-off attack nodes by employing Predictability Trust to recognize a pattern of malicious behaviors.
- To provide a mechanism to allow designers of distributed systems that employ this trust management scheme to choose an acceptable level of risk for their particular applications.

In this dissertation work we are proposed the New modified Trust Management Frame for on –off attack for the Wire less sensor network. In this frame work we are indentified the bad behavior node during the massages sending using detecting the neighboring on –off nodes detection technique that is Bayesian formula.

1.10 Figure Screen shots of Implemented System

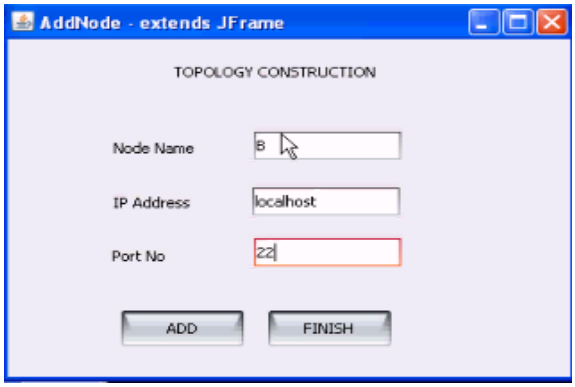

Figure1.4 Different Node Creation

Figure 1.5 Packet path construction with weight (A)

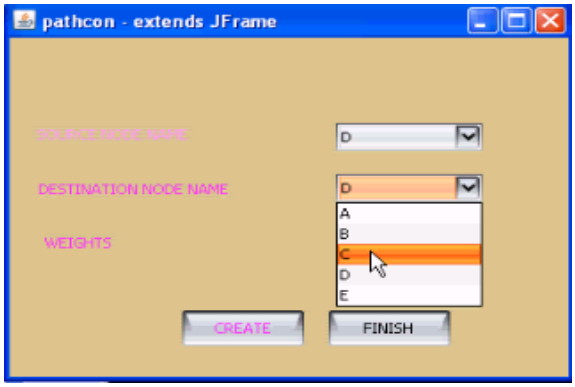

Figure 1.6 Packet path construction with weight (B)

REFERENCE:

[1] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," Computer. Communication, vol. 33, no. 9, pp. 1086–1093, 2010.

[2] I. Akyildiz, W. Su, Y. Sankara Subramaniam, and E. Cayirci, "Wireless sensor networks: A

survey," Computer. Network, vol. 38, no. 4, pp. 393–422, 2002.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior BB in mobile ad hoc networks," in Proc. 6th Annual International Conference Mobile Computer Network., 2000, pp. 255–265.

[4] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43, no. 2, pp. 618–644, 2005.

[5] M. Langheinrich, "When trust does not compute – the role of trust in ubiquitous computing," in Proceedings of the 5th International Conference on Ubiquitous Computing (UBICOMP), Seattle, Washington, October 2003.

[6] A. Perrig, D. Clark, and S. Bellovin (Editors), "Secure next generation internet," NSF Workshop Report, July 2005.

[7] Y. Sun, W. Yu, Z. Han, and K. J. Ray Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE JSAC Special Issue on Security in Wireless Ad Hoc Networks, vol. 24, pp. 305– 317, February 2006.

[8] https://www.paloaltonetworks.com/resources/learning-center/what-is-cyber-security.html

[9] http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm

[10] http://www.itgovernance.co.uk/what-is-cybersecurity.aspx#

[11] https://dict.mizoram.gov.in/uploads/attachments/cyber_crime/intro-indian-cyber-law.pdf

[12] http://www.cybersecuritycrimes.com/types-of-cyber-attacks/

* * * * *