A Survey on Securitization of Internet Governance with Proper Trust Management Form On- Off Attack in WSN Domain

Sumit Pathak[1]
[1](Computer Science & Engineering , RGPV, Jabalpur, India ,rohanback@gmail.com)

Abstract—*I This is the Survey paper of Trust Management System over the Internet, in this paper we are study the various application of Trust management ,its advantages, a simple working concept of Trust management System. Today maximum research papers on are used the internet facility for the various purpose , but person is not aware related to security related information a internet user easily trust the service provide by the service provider , in the other word we can say that person are easily trust on the service provider for any kind of service related to internet like emailing , transition etc. so this paper is A survey paper based on the Securitization of Internet Governance with Proper TMS for the Different kind of ON-OFF Attack (OOA). In this paper we are include the some information Related to OOA.*

Keywords— *Trust Management, cyber Security Attack , WSN, Redemption Technique ,Control Policy ,Vulnerabilities .*

1.INTRODUCTION OF CYBER CRIME

Cybercrime [1] is a range of illegal digital activities targeted at organisations in order to cause harm. The term applies to a wide range of targets and attack methods. It can range from mere web site defacements to grave activities such as service disruptions that impact business revenues to e-banking frauds. The first cybercrime was noted in 1820 by Joseph-Marie Jacquard, a textile manufacturer in France which produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. In the past, India used to be a target of cyber attacks for political motivation only. Over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent. These attacks, which were rarely malicious, have gradually evolved into cybercrime syndicates siphoning off money through illegal cyber channels.

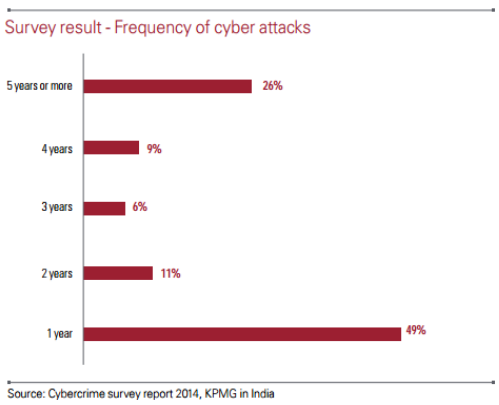

Figure 1.1 Cyber Attacks

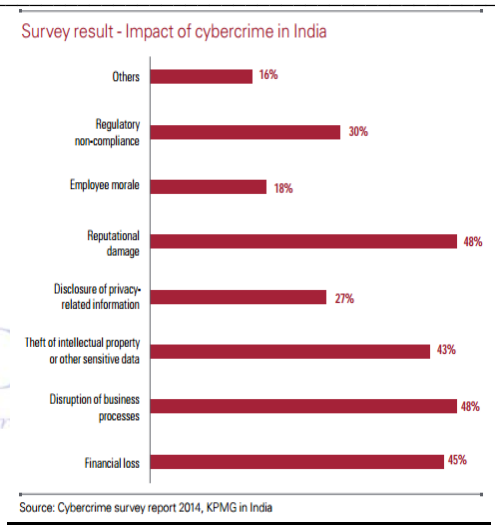

Figure 1.2 Cyber Crime in India

Cyber attacks [1] by their very nature are multi-dimensional and complex. As cybercrime progressively evolves into an organized activity, the motives of intruders are no longer limited to stealing information only, but potentially to disrupt business or conduct espionage on behalf of competing organisations. Although organisations understand the need to safeguard their IT infrastructure, intruders have often been a step ahead at exploiting new vulnerabilities in IT systems and processes of their target. Needless to say, target organisations have been found wanting when it comes to countering these cyber attacks.A cyber attack [2]is an assault by a third party via a computer against another computeror computer system, which is intended to compromise the integrity, availability or confidentiality of that computer or computer system. For example:

• A remote attack on a business's IT systems or website.

• Attacks on information held in third-party systems (for example, the company bank account).

2.TRUST MANAGEMENT SCHEME

Trust is the probability that an object performs a given action as expected. A trust management scheme manages the trust by integrating the notions of credentials, access control, security policy, availability, and authentication. By using the integrated information, a trust management scheme can be used to aid an automated decision making process for an access control policy. Trust can be evaluated in a variety of ways. Direct observation evaluates neighboring nodes by observing their behavior. For example, in a WSN, a node is able to detect malicious neighbors by monitoring how many packets were forwarded to the next node. Moreover, if a source node compares the contents of the packets, it can detect fabrication or modification. With indirect observation nodes publish their direct observations to their neighboring nodes to warn about malicious nodes or to report recovered nodes that were previously evaluated as malicious. In a WSN, a warning message from other nodes will exclude the malicious node from the network. On the other hand, recovery reports from other nodes can allow nodes to rejoin the network. Trust evaluations can also be disrupted. In a WSN, a direct observation can be disrupted by network fault. When a node monitors the forwarding performance of its neighboring node, network fault may cause the packets to be lost on their way to the monitoring node even if the all of the packets were successfully delivered to the forwarding node. An indirect observation can be disrupted by bad mouthing. An attack node may frame other normal nodes to make them look like malicious nodes, or may recover the trust of a malicious node by reporting false praises. To avoid faulty detections, direct observation can employ a trust redemption scheme, and indirect evaluation minimizes the influence of the warning messages or reports.

The unique characteristics of wireless sensor networks make them susceptible to the attacks. The secure scheme is considered in designing the routing protocol and algorithm. The cryptography and authentication secure technology can defend the external attacks but have no way to protect the network when the internal attacks occur. However, the trust management scheme with attack-resistance and robustness can efficiently detect the internal attack. On the condition of defending the attacks, it is also an issue that the trustmanagement scheme aids routing algorithmto improve the security and performance. In this paper,we proposed a Trusted Tree-based trust management for secure routing in wireless sensor networks. The common attacks are firstly analyzed. And then the dynamic time window is designed in the distributed trust model with the detection of direct trust and indirect trust.Based on the trusted nodes, Trusted Tree [3] is constructed. And the path quality of nodes in Trusted Tree is used as the gradient for routing. Finally, we add Trusted Tree-based trust management into the QoS based routing protocol and algorithm .

3.ON-OFF ATTACK

A smart attacker may attempt to disturb a trust redemption scheme by behaving well and badly alternatively so that trust is always redeemed just before another attack occurs. This type of attack is referred to as an On-off attack [4]. Most trust redemption schemes fail to effectively discriminate between an On-off attack and temporary errors, especially when the majority of the attacker's behavior is good. Therefore, an attacker may be able to remain active in the system by disguising the attacks as temporary errors. In general, if the malicious node performs n good behaviors and m bad behaviors alternating, refer to this as an nG-mB On-off attack. For example, 4G-1B attack node means the node behaves well four times and behaves badly one time alternatively.

This can also be called a 80 percent G-20 percent B On-off attack. An On-off attack does not work alone, but associates with another type of attack. For example, a malicious node in a WSN may associate a selective forwarding attack with the On-off attack where most of the time it forwards all packets but occasionally it drops most or all of the packets. There are two states in an On-off attack; the On state and the Off state. An On state is referred as an attack state. When a malicious node is in the On state, the node attacks the target nodes with the associated attack. An Off state is referred to as a normal state. When a malicious node is in an Off state, it behaves normally. When the ratio of the Off state to On state is high, the trust management system may have difficulty detecting the malicious behaviors. There is a tradeoff for the attacker between remaining active in the system and performing highly efficient attacks. The higher the Off-to-On ratio, the longer the attacker can remain in the system, but the less efficient the attack. The authors investigated the On-off attack by combining a packet dropping attack with a simple On-off attack, such as 1:1, 2:1, and 3:1 Off-to-On ratio. The attack was launched against first-hand observation based reputation schemes like OCEAN, and they showed the hiding ability of On-off attacks in their simulations. The authors reinforced a Denial of Service (DoS) attack by employing On-off attack. They showed the vulnerabilities of the Directed Diffusion protocol in WSN to the On-off attack.

4.ON-OFF ATTACK DEFENSE

There exist trust management schemes that address On-off attack in various types of networks, such as Traditional Networks, Cognitive Radio Networks, Peer-to-Peer Networks, Ad-hoc Networks, and Wireless Sensor Networks. However, no trust management scheme is able to discriminate between temporary errors and On-off attacks.The authors propose evaluating neighboring nodes by using direct and indirect trust values. The solution described, uses a compilation of direct and indirect evaluations to reduce the trust of an On-off attacker to be lower than the trust of other neighboring normal nodes, so the network will detour around the On-off attack nodes in the system. However, in the simulation, they did not consider when a source node was surrounded by malicious nodes and had only one normal path to traverse. Therefore, since there were many good options to take, the On-off attacker did not have an opportunity to continue its attack. In our work, we have considered a harsher WSN environment in which a node may be surrounded by malicious nodes and only have one possible normal path to the base station.The scheme described, also used an integration of direct and indirect evaluation to reduce the

trust of an Onoff attack to be smaller than a threshold. The trust management scheme was tested in a simulation against an On-off attack with 50 good behaviors and 50 bad behaviors, thus with an Off-to-On ratio of 1:1. This is a rather simple On-off attack that can be easily detected because it is hard to disguise the bad behaviors as temporary errors and because it has many bad behaviors in succession. Moreover, since both of these trust management schemes employ TBR, there still exists the risk to recover the trust of an On-off attack node to greater than the threshold. This scheme was not tested against more sophisticated On-off attacks with lower Off-to-On ratios. Our work considers various Off-to-On ratios. The authors provide a defense against On-off attack by reducing the trust drastically when they detect an error. This scheme defends against an On-off attack with the drastic trust decrement and slow recovery with a small forgetting factor. However, since this trust management scheme employs a BBR with a forgetting factor, it is not able to recover the trust of a malicious node because there is no further observation. Each node periodically sends a special type of packet, called a PROBE that detects an On-off attack while the attack is in an On state. If the period of PROBE packets is not short enough, this scheme is not able to detect the Onoff attack. However, if the period of PROBE packets is short enough, it might detect the On-off attack, but it would consume a lot of resources. Moreover, can only detect when an On-off attack changes the behavior based on time, but cannot detect when an On-off attack changes the behaviors based on the number of good or bad behavior .Various Redemption Technique of Cyber Attack – A List of Various Redemption Technique are shown the Table .

S.No	Redemption Technique Name	Description
1	Use Strong Passwords	Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.
2	Secure your computer	• Activate your firewall • Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers. • Use anti-virus/malware software.
3	Be Social-Media Savvy	Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!
4	Secure your Mobile Devices	Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.
5	Install the latest operating system updates	Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

Table Various Redemption Technique

5.BEHAVIOR BASED REDEMPTION

To understand Behavior Based Redemption, assume that a friend had a bad behavior in the past, but since then the friend has behaved very well several times. Thus, we can expect that the friend will behave well in the next behavior. Similarly in a distributed system, if a node behaves very well now, we can expect the node will behave well in the next behavior, even if the node had a bad behavior in the past. A representative scheme is presented in CORE. CORE evaluates neighboring nodes based on direct observation, indirect observation that considers only positive reports by others, and task-specific behavior. These are compiled by a weighted trust technique, and the compiled result is used for discriminating and isolating a malicious node from the network. CORE assigns higher weight to past behaviors than recent behavior to minimize the influence of a recent bad behavior on the evaluation. Note that BBR is not a very good choice of redemption technique for systems in which nodes are isolated from use when trust is low, because BBR relies on subsequent behaviors to allow trust to be redeemed. Since trust is used to make decisions about collaboration, an untrusted node will not have a chance to participate in the network, and therefore no new behaviors can be observed. We discuss this type of redemption scheme because it is a widely used technique for trust redemption in general, especially when a scheme employs beta reputation system.

6.TIME BASED REDEMPTION

If we assume that a friend had a bad behavior in the past, we might decide not to trust the friend for a while. After time has passed, we may expect the bad behavior was a mistake, and give the friend another chance. This represents Time Based Redemption. We provide some time to a node to recover from a temporary error, and we give another opportunity to behave well. For example, OCEAN is a method proposed. In OCEAN negative behavior decreases the rating of the node more than positive behavior increments the rating. When the rating is below a threshold, the node is added to the faulty list, and the faulty list is broadcast. Other nodes use this faulty list to avoid the malicious nodes. OCEAN removes a node from the faulty list by using a timeout-based approach. Sometimes TBR is referred to as an aging technique. However, TBR alone does not consider the next behavior in the context of past behaviors, so a node's trust is recovered no matter how badly it behaved in the past. TBR is usually used for supplementing BBR. CONFIDANT is another method, which adapts a Bayesian reputation system with weighted trust evaluation (BBR). It also uses TBR by using a fading technique that discounts all ratings periodically and upon observation by exponential decay. While the trust redemption schemes described above pro-vide the ability for a node's trust to be redeemed, each of these is vulnerable to an On-off attack, because they are not able to recognize the malicious pattern.

Vulnerability[5]: if computer security is applied to a weakness in a system which allows an attacker to violate the integrity of that system. This weakness of an asset or group of assets can be exploited by one or more threats. Vulnerabilities may result from different reasons such as weak passwords, software bugs, a computer virus, other malware, script code injection or a SQL injection. Information security tasks are all related to managing and reducing the risks related to information usage in an organization, usually, but not always, by reducing or handling vulnerabilities or threats. Thus, it is wrong to think of security in terms of vulnerability[5] reduction. Security is a component of the organizational risk management process; a set of coordinated activities to direct and control an organization with regard to risk. In other words, information security is the protection of

information from a wide range of threats in order to ensure continuity, minimize risk, and maximize return on investments and business opportunities. The main phases of a proper security risk recovery are:

Risk analysis/assessment: process of analyzing threats and vulnerabilities[5] of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures. It is the systematic use of information to identify risk sources and to estimate the risk;

Risk evaluation: the process of comparing the estimated risk against given risk criteria to determine the significance of the risk;

Risk management: Process concerned with the identification, measurement, control, and minimization of security risks in information systems.

Reference

[1]https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf

[2] Cyber security: business briefing

[3] Trusted Tree-Based Trust Management Scheme for Secure Routing in Wireless Sensor Networks Zhi Hu,1,2 Yuxia Bie,3 and Hong Zhao1,2 1College of Information Science and Engineering, Northeastern University, Shenyang 110819, China 2Software Centre, Northeastern University, Shenyang 110819, China3Information College, Dalian University, Dalian 116622, China

[4] Research Article Mitigating On-Off Attacks in the Internet of Things Using a Distributed Trust Management Scheme Carolina V. L. Mendoza and João H. Kleinschmidt

[5] Defense of Trust Management Vulnerabilities in Distributed Networks Yan (Lindsay) Sun¤, Zhu Hany, and K. J. Ray Liuz ¤ Department of Electrical and Computer Engineering University