Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.233 – 241

RESEARCH ARTICLE

DETECTING AND RESOLVING THE SYBIL ATTACK IN MANET USING RSS ALGORITHM

K.Vaijayanthi*, M.Baskar, M.Sc., M.Phil.**
*M.Phil(Computer Science), Research Scholar,
Vivekanandha College for Women, Unjanai, Tiruchengode, India
******Assistant Professor in Computer Science
Vivekanandha College for Women, Unjanai, Tiruchengode, India

ABSTRACT: ***The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc Network (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. The propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly affect the network performances.***
Keywords: RSS Algorithm, RSS Detection Mechanism, Sybil Attacks, MANET

1. INTRODUCTION

Mobile computing offers significant benefits for organizations that choose to integrate the technology into their fixed organizational information system. Mobile computing is made possible by portable computer hardware, software, and communications systems that interact with a non-mobile organizational information system while away from the normal, fixed workplace. Mobile computing is a versatile and potentially strategic technology that improves information quality and accessibility, increases operational efficiency, and enhances management effectiveness. Mobile computing is accomplished using a combination of: (a) computer hardware; (b) system and applications software; and (c) some form of communications medium. Powerful mobile solutions have recently become possible because of the availability of: (a) extremely powerful and small computing devices; (b) specialized software; and (c) improved telecommunications

1.1 ROUTING ATTACKS IN MANET

Routing plays a very important role in MANETS. It can also be easily misused, leading to various types of attack in the network. Routing protocols in general are more easily attacked by malicious nodes. These protocols are usually not designed with security function and often they are very vulnerable to node misbehavior attacks. It is true for MANET routing protocols because they are designed for minimizing the level of overhead and for allowing every node to participate in the routing process.

Various routing attacks caused by attackers in MANET are:

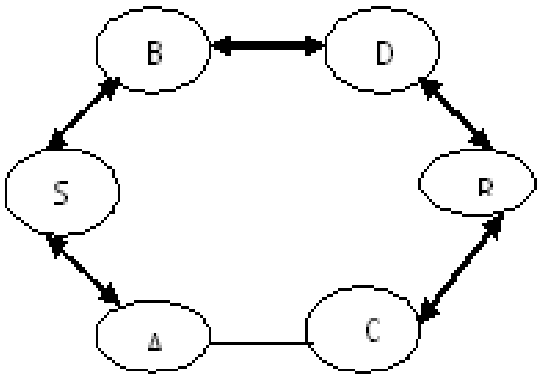
Wormhole Attack

In wormhole attack, an attacker receives a packet at one point and tunnels it to another malicious node in the network. This way beginner assumes that he found the shortest path in the network. This tunnel between two colluding attackers is called the wormhole.

Black hole Attack

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply

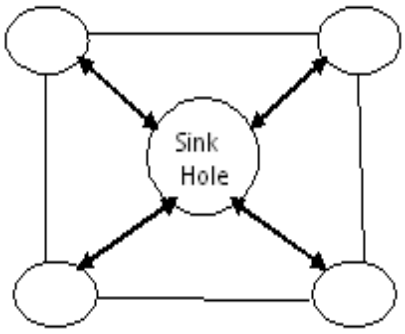
reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.



Black hole Attack

Sybil Attacks

Sybil attack refers to the multiple copies of malicious nodes. It can be happen, if the malicious node shares its secret key with other malicious nodes. This way the number of malicious node is increased in the network and the probability of the attack is also increased. If we use the multipath routing, then the possibility of choosing a path in the network, those contain the malicious node will be increased.



Sybil Attack

Flooding Attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

Malicious code attacks

Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

Masquerading Attacks

During the neighbor acquisition method, an outside intruder might masquerade a nonexistent or existing IS (Information Systems) by attaching itself to communication link and illegally joining in the routing protocol domain by compromising an authentication system. The threat of masquerading is almost the same as that of a compromised IS.

2. LITERATURE SURVEY

I.Chlamtac, M. Conti, And J. J.-N. Liu This paper attempts to provide a comprehensive overview of this dynamic field. It first explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies. Then, it reviews the latest research activities in these areas of MANET characteristics, capabilities and applications. J. Newsome, E. Shi, D. Song, And A. Perrig It establish a classification of different types of the Sybil attack, which enables us to better understand the threats posed by each type, and better design countermeasures against each type. To propose several novel techniques to defend against the Sybil attack, and analyze their effectiveness quantitatively. Y. Chen, J. Yang, W. Trappe, And R. P. Martin Our results show that it is possible to detect wireless identity-based attacks with both a high detection rate and a low false-positive rate, thereby providing strong evidence of the effectiveness of the attack detector utilizing the spatial correlation of RSS and the attack localizer.

3. METHODOLOGY

3.1 RSS METHOD

In an IEEE 802.11 system, RSSI is the relative received signal strength in a wireless environment, in arbitrary units. RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal. RSS can be used internally in a wireless networking card to determine when the amount of radio energy in the channel is below a certain threshold at which point the network card is clear to send (CTS).

Once the card is clear to send, a packet of information can be sent. The end-user will likely observe a RSSI value when measuring the signal strength of a wireless network through the use of a wireless network monitoring tool like Wireshark, Kismet or Inssider. As an example, Cisco Systems cards have a RSSI Max value of 100 and will report 101 different power levels, where the RSSI value is 0 to 100. Another popular Wi-Fi chipset is made by Atheros. An Atheros based card will return an RSSI value of 0 to 127 (0x7f) with 128 (0x80) indicating an invalid value.

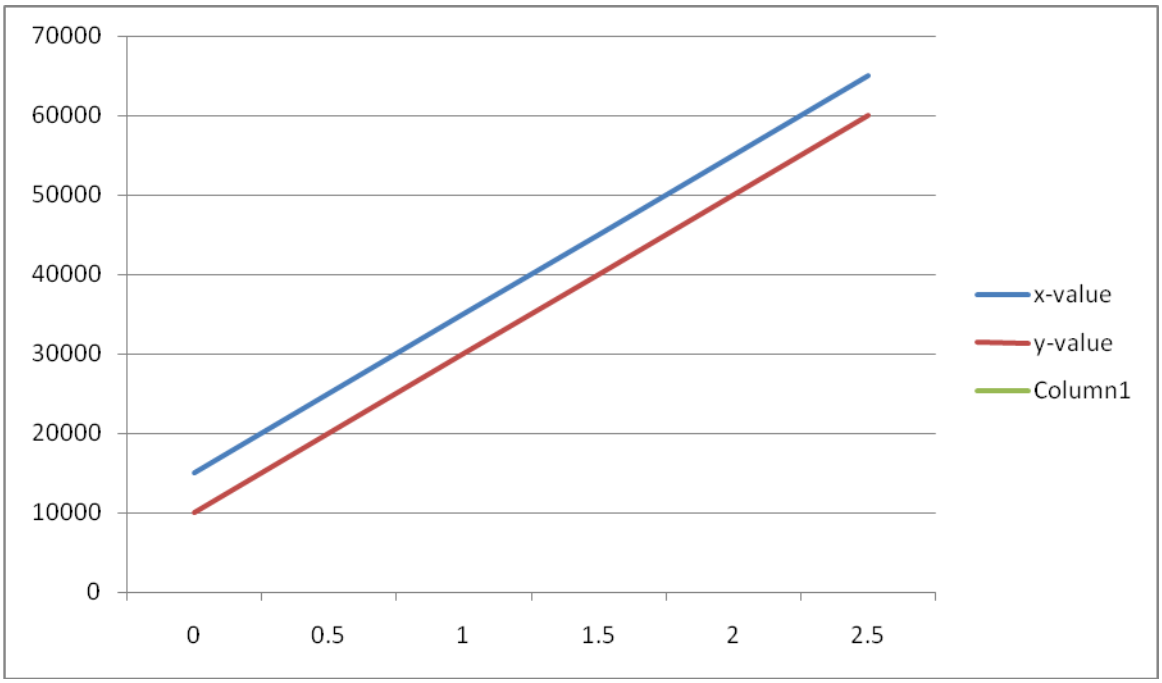
3.2 RSS DETECTION MECHANISM METHOD

This paper proposes a mechanism for detecting session hijacking attacks in wireless networks. The proposed scheme is based on using a wavelet based analysis of the received signal strength. The first develop a model to describe the changes in the received signal strength of a wireless station during a session hijack, while the received signal is embedded in colored noise caused by fading wireless channels. An optimal filter is then designed for the purpose of detection. Show that using a Wavelet Transform (WT), the colored noise with complex Power Spectral Density (PSD) in our case can be approximately whitened. Since a larger Signal to Noise Ratio (SNR) increases the detection rate and decreases the false alarm rate, the SNR is maximized by analyzing the signal at specific frequency ranges.

The detection mechanism is validated using both simulation and experimental results. The detector is shown to be reliable, computationally inexpensive and have minimal impact on the network performance.

4. EXPERIMENTS RESULT

The report an experimental test of the RSS detection mechanism in a nanowire superconducting single photon detector. Detector tomography allows us to explore the 0.8–8 eV energy range via multiphoton excitations. High accuracy results enable a detailed comparison of the experimental data with theories for the mechanism of photon detection. Show that the temperature dependence of the efficiency of the superconducting single photon detector is determined not by the critical current but by the current associated with vortex unbinding. Find that both quasiparticle diffusion and vortices play a role in the detection event.

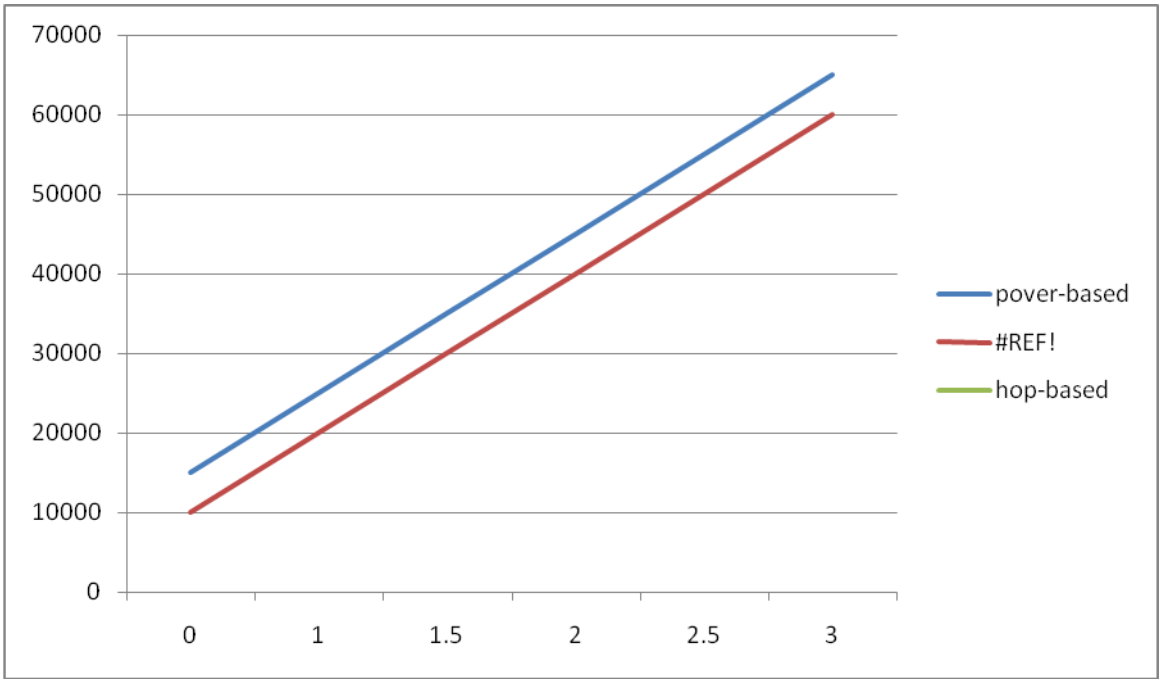


SSO PERFORMANCE LEVEL ON ROUTING

A set of experiments has been constructed to demonstrate control strategies for a single-link, very flexible manipulator, where the position of one end is to be sensed and precisely positioned by torquing at the other end. The objective of this first set of experiments is to uncover and solve problems related to the control of very flexible manipulators where sensors are not colocated with the actuator. The experimental arrangement described here is also a test bed for new designs for flexible-structure controllers, designs that use insensitive, reduced-order

control and adaptive control methods, for example. This paper describes the experimental arrangement, model identification, control design, and first experimental results.

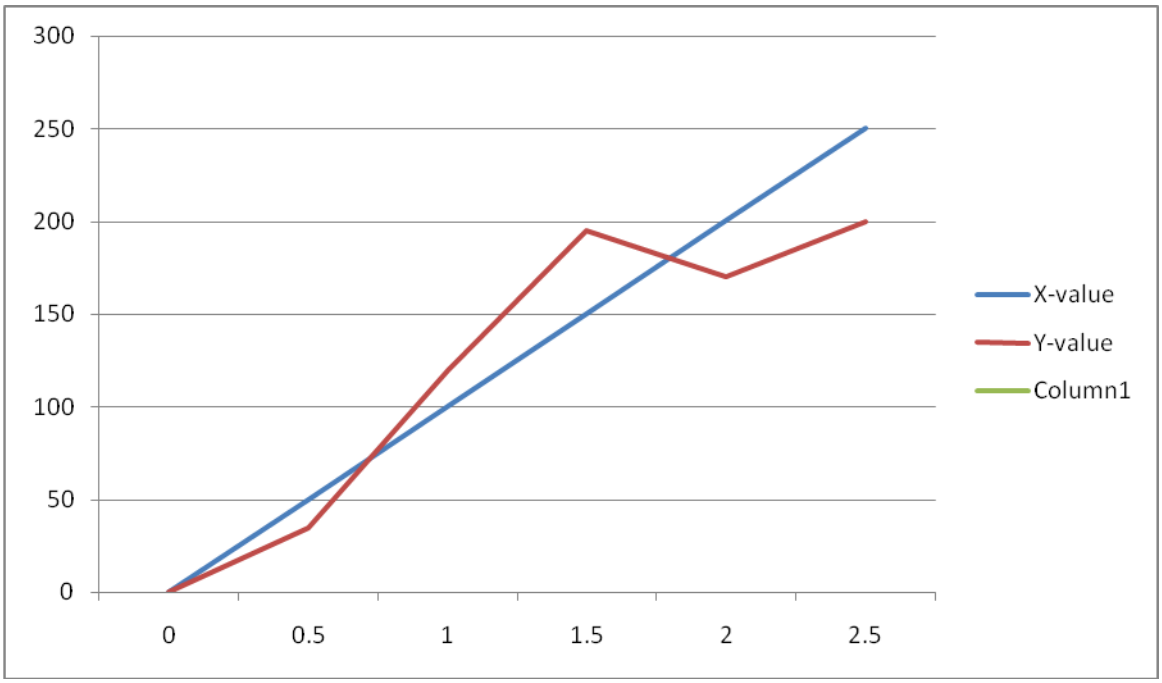
Some interesting results are the following. First, good stability can be achieved for such noncolocated systems, and response can be achieved that is effectively three times faster than the first natural cantilever period of the system: but a good model of the system dynamics and rather sophisticated control algorithms are essential to doing so. Even then, the system will always be conditionally stable. In addition to the tip sensor, a colocated rate sensor and nearly colocated strain gauges have been found to be very useful for achieving good closed-loop performance, that is, high gain and high band width.



PERFORMANCE LEVEL1

Second, there is an ultimate physical limit to achieve able response time, namely, the time required for a wave to travel the length of the member. Well-designed controllers can approach this limit. Third, the use of end-point sensing makes less critical the elaborate dynamic conditioning of position-command signals "model-following " differentiators, feed-forward, and

the like such as are typically needed in present-generation robots that use "dead reckoning" in lieu of end-point sensing.



PERFORMANCE LEVEL 2

With end-point sensing, feedback alone *(*suitably conditioned*)* is sufficient to whip the tip to the commanded position and hold it there precisely. Even more important, a shift in, for example, work piece with respect to robot base, no longer produces an error.

5. CONCLUSION & FUTURE ENHANCEMENTS

The proposed a risk-aware response solution for mitigating MANET routing attacks. Especially, our approach considered the potential damages of attacks and countermeasures. In order to measure the risk of both attacks and countermeasures, and extended Dempster-Shafer theory of evidence with a notion of importance factors. Based on several metrics, also investigated the performance and practicality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our risk aware approach. Based on the promising results obtained through these experiments, the would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model. The

Feature is a probabilistic rebroadcast protocol based on neighbor coverage to reduce the routing overhead in MANETs. This neighbor coverage knowledge includes additional coverage ratio and connectivity factor. Proposed a new scheme to dynamically calculate the rebroadcast delay, which is used to determine the forwarding order and more effectively exploit the neighbor coverage knowledge. Simulation results show that the proposed protocol generates less rebroadcast traffic than the flooding and some other optimized scheme in literatures. Because of less redundant rebroadcast, the proposed protocol mitigates the network collision and contention, so as to increase the packet delivery ratio and decrease the average end-to-end delay. The simulation results also show that the proposed protocol has good performance when the network is in high density or the traffic is in heavy load. Future work is in progress to consider dynamic traffic patterns in the proposed scheme to further improve the performance of MANETs with cooperative communications.

REFERENCES

[1] National Institute of Standards and Technology (NIST), **"NIST Debuts New Approach To Ad Hoc Networks For First Responders,"**

[2] The National Oceanic and Atmospheric Administration (NOAA), **"NOAA Unmanned Aircraft System,"**. Last accessed April 2009.

[3] S. Hashmi and J. Brooke, **"Toward Sybil Resistant Authentication In Mobile Ad Hoc Networks,"** in Proc. 4th Int. Conf. Emerging Security Inform., Syst. Technol., 2010, pp. 1724.

[4] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, **"Detecting And Localizing Identity-Based Attacks In Wireless And Sensor Networks,"** IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[5] I. Chlamtac, M. Conti, and J. J.-N. Liu, **"Mobile Ad Hoc Networking:Imperatives And Challenges,"** *Ad Hoc Netw.*, vol. 1, no. 1, pp. 13–64,2003.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig, **"The Sybil Attack In Sensor Networks: Analysis And Defences,"** presented at the 3rd Int. Symp. Information Processing in Sensor Networks (IPSN), 2004, pp. 259–268

[7] K. Hoeper and G. Gong, **"Bootstrapping Security In Mobile Ad Hoc Networks Using Identity-Based Schemes,"** in *Security in Distributed and Networking Systems* (Computer and Network Security). Singapore: World Scientific, 2007

