Increase Wireless Network Security Using W-LAN Algorithm and W-WAN Database

K.A.L.K.Dhananjaya Arachchi, K.A.D.K.N.Peiris, M.Nishanthan, I.D.M.D.Sandimali, R.Indrakumar, W.A.L.K.Athukorala, U.G.P.R.Weeragoda and Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology (pvt) Ltd

Abstract- Wireless Local Area Network (W-LAN) security has signified incredible favorable advantages in numerous fields, with adaptable and straightforward access, W-LAN system administration has an extensive variety of requisition. This project involves the implementation of a network with more security by using measures which will disable access for unauthorized users to the network. The goal is to rise W-LAN security by introducing a W-LAN management system which can prevent the intruders who are try to access the system for steal the data. For this security process system going to detect the intruders and categorize them by using the algorithm and using data mining techniques, after categorizing system check activities of that devices and if the system feel that the activities are harm then it will block the device permanently from that network system. Although considerable debate exists regarding the risks and benefits of building a W-LAN it is possible to reduce unauthorized access to the system by making use of the existing technologies while building protocols to add more. Spoofing, Eavesdropping, phishing and other methods of accessing the network can be eliminated by this particular system.

Index Terms- Wireless local Area network, Wireless Wide Area Network, W-LAN Algorithm, Wireless LAN Security, W-LAN Database.

I. INTRODUCTION

W-LAN is becoming a common part of today's business organizations. The benefit of W-LAN connectivity for organizations includes elasticity, convenience, increased productivity, relatively low costs and ease of implementation. It can also serve to improve the effectiveness and excellently of the external audit for both the organization and the auditor and also most of computers sold to users today come pre-equipped with all necessary wireless Networks technology. As the technology continues to improve, the price of wireless services and hardware, such as laptop computer and other mobile devices, keeps trending down. Today, many mobile workers use mobile devices far beyond e-mail. Increased storage capacity and by using internet connectivity mobile workers can store huge amounts of private critical data and to access the corporation's back-end system remotely. Wireless communication nowadays becomes companies' intentional tool to gain competitive advantage. Companies gain profits to improve the connectedness of a workforce and to enhance decision making process by providing quicker access to more present information. Wireless communication also improves workers' satisfactory and productivity by providing easier and flexible access option.

Still, along with these benefits, wireless communication also adds security risks to the integrity of the company's network. The more immediate concerns for wireless communications are device theft, denial of service, malicious intruders, harmful code, theft of service and industrial, access control risks. Theft is likely to occur with wireless devices because of their portability. Authorized and unauthorized users of the system may obligate fraud and theft; however, approved users are more likely to carry out such acts. Since users of a system may recognize what resources a system has and the system's security flaws, it is easier for them to commit fraud and theft. Harmful hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for individual advantage or to do harm. Malicious hackers are generally individuals from outside of an agency or organization. Such intruders may gain access to the wireless network access point by eavesdropping on wireless device communications. Harmful code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or bring down a system.

This paper will cover the part of risk that are facing when accessing to the private Wi-Fi network Unlike the traditional network, wireless network use electromagnetic radiation as their means of transmitting data through space. Access control is a famous security mechanism to give right of entry permission or denial message to an access request according to the predefined access guidelines, in which the system monitors and controls who can access the precise data and also what they can do onto that data.

This paper proposes a way to secure the access of a particular user. Whether the user is an intruder or not. Our proposed method will first detect and analyze the particular user that is connected to the network and categorize the user to a harmful user or not, according to user's behavior in the network and from the previous stored recordings. According to the records if the particular user is harmful, system will automatically send the user to a public network and will block the access using the user's mac address. If the user is not a threat to the system will grant the access and both accesses will be stored in the log. To store details and retrieve data, system will use Syslog. Syslog is the way for network devises to send event messages to a logging sever. The Syslog protocol is supported by a wide range of devices and can be used to log different types of occasions. For example, a router might send messages about users logging on to support sessions, while a web-server might log access-denied events.

Using the syslog, system will analyze the pattern that how will the intruders will attack the network and will analyze the time period of the attacks and by analyzing those will prevent and secure the network.

I. Wireless Security risks, Detection and Prevention

Wireless security risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity, some are new. The most significant source of risks in wireless networks is that technology's underlying communication medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot. In order to detect and prevent these attacks any methods have been developed. The study of those researches will be as follows

a. Research Issues and Challenges of Wireless Networks

Wireless networking presents many advantages Productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications take place

"Through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The objective of this paper is to assist managers in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networking and available countermeasures. [2][3]

a.a. Wireless Local Area Network

Wireless LANS provides details over view of 802.11 frequency range wireless technology. This has introduced the history of 802.11 technical information, network technologies and transmission range. It tests the security threats and vulnerabilities associated with wireless LANS and reducing risks of security WLANS environment.

Motorola developed one of the first commercial WLAN systems with its Altair product. However, early WLAN technologies had several problems that prohibited its pervasive use. Those were much LANs expensive, provided low data rates, were prone to radio interference, and were designed mostly to proprietary RF technologies. The IEEE initiated the 802.11 project in 1990 with a scope "to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area." In 1997, IEEE first approved the 802.11 international interoperability standard. Then, in 1999, the IEEE ratified the 802.11a and the 802.11b wireless networking communication standards. The goal was to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications. The 802.11a standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference. This technology uses the 5 GHz frequency spectrum and can process data at up to 54 Mbps.

a.b. Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET)

Mobile Ad Hoc Network (MANET) is the kind of wireless networks which don't require any fixed Infrastructure or base stations or in or we can say it as Mobile Ad Hoc Network, these are collection of wireless mobile Communication devices or nodes communicating with other without any fixed infrastructure or federal administration. The nodes in MANET themselves are responsible for searching out other nodes to communicate with dynamism. In MANET, it may be necessary for one wireless mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each wireless mobile node operates not only as a host but also as a router forwarding packets for mobile nodes which has wireless network that may not be within the direct transmission range of each other. Every node take part in an ad hoc routing protocol that allows it to discover multi-hop paths through the network for other node. This wireless networking of Mobile ad hoc network type is also called infrastructure less networking, since the mobile nodes in the network establish routing to form their own network by themselves on the fly, dynamically [6]. Figure 1 illustrate the structure of mobile Ad Hoc Network.

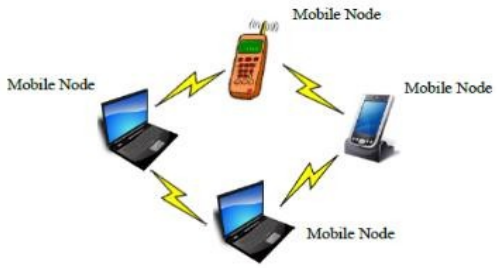

Figure 1: Structure of Mobile Ad Hoc Network (MANET) Source: A Survey on Routing Protocol and vulnerability in Mobile Ad-Hoc Network (MANET) Research Paper

a. Wireless Mesh networking security

Mesh networking is configuration of peer wireless access nodes that allow for continuous connections to a network infrastructure, including reconfiguration around blocked paths, by "hopping" from node to node. There are many different types of wireless mesh security architectures, where each type of architectures may use a different approach for wireless security. Many approaches for mesh security may be derived from ad-hoc security research, but any future commercial mesh products will standardize security through 802.11s

b.a. Ad-hoc Security and Research

Message integrity protection using public/private key security, including transitive trust architectures, between routing peers (SUCV), or message authentication using hash chains to

ensure detect tampering of routing information within the network (SEAD); Authentication of routing messages using digital certificates (SAODV); and, Protection by symmetric cryptography, using shared secrets or digital signatures (Ariadne).

b.b. Standardization

Standardization activities for security will focus on inter-AP security controls, where client access uses standard WPA2/802.11i authentication and encryption.

Standardization on security between mesh access points is still being finalized within the standard. However, link-by-link security mechanism will be based on 802.11i, with a security Architecture based on 802.1X authentication.

Mesh APs may have supplicant, authentication and authentication server roles. EAP 4-way handshakes must occur between all mesh routing peers, where centralized 802.1X authentication is supported. However, means of communicating between authentication server and remote mesh AP is presently not within the scope of the standard the 802.11r standard for client mobility influences the security architecture by enabling a hierarchical key distribution scheme to improve mesh route maintenance.

Specifically, this means leveraging key hierarchies and co-ordination with a central/trusted key-holder for pair-wise master keys (e.g., an AP acting as an authenticator will need the pair-wise master keys of the supplicant AP to generate session/transient keys prior to the EAP 4way handshake). [1] Figure 2 illustrate the wireless mesh authentication and encryption.

.

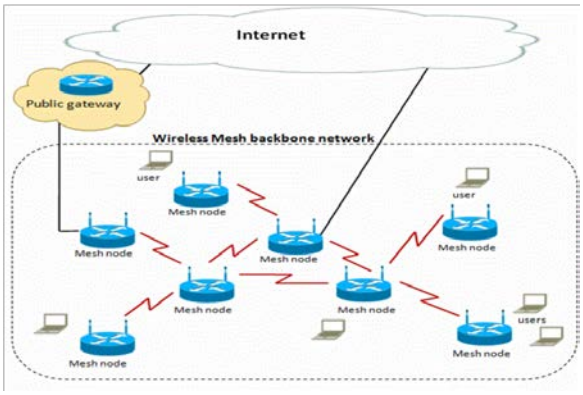

Figure 2: Wireless mesh authentication and encryption

Source: http://wiki.mikrotik.com/images/1/1b/image14002.gif

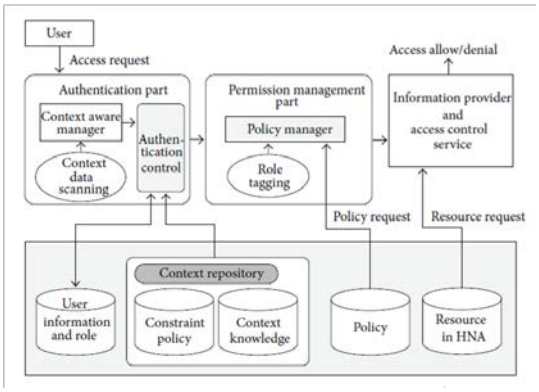

Figure 3: Overview of dynamic access control Model.

Source: Dynamic Access Control Model for Security Client SeeVices in Smart GridResearch paper

c. Host base intruder detection and prevention systems

c.a. Dynamic Access Control Model for Security Client Services in Smart Grid

Dynamic Access Control Model for Security Client Services in Smart Grid, this research paper about dynamic access model for secure user services in the smart grid environment. Access control is a well-known security mechanism to give access or denial message to an access request and the system monitors and control who can access the specific data and also what they can do that data. Dynamic access control uses place, time and purpose according to context information as the conditions for access permission. This research is done by Sang-Soo Yeo, Si-Jung Kim and Do-Eun Cho. In the intelligent power grid, various objects can access system in several network environments so access control security becomes critical. In this research paper create new access control security model to provide users with secure services in the smart grid. This model analyzes the user's various access contexts and chooses an appropriate context type among the predefined context types. And then it applies the context-based user security policy to allow the user's access to services dynamically. It provides stronger security services by permitting context information applied security services and flexible access control in various network environments. Using this system solve important access control issues when establishing the smart grid. [10] Figure 3 illustrate overview of Dynamic access control model.

c.b. Detecting and Eliminating Rogue Access Points in Ieee-802.11 Wlan -A Multi-Agent Sourcing Methodology.

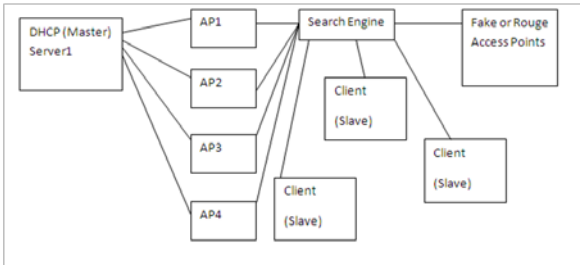

Figure 4: System architecture
Source: Detection and Elimination of Fake Access Points in WLAN using Multi Agents and Clock Skew Methodology research paper.

The master and slave agents are spontaneously look over the networks for any unauthorized access points using the skew intervals. Initially a master agent is generated on the DHCP-M server, which is responsible for regulating all the authorized processes of the Wireless Network.

This Master Agent generates slave agents depends upon the number of active Access Points Connected to the Server at that moment of time.

These slave agents are then transmitted on the respective APs connected.

Now these slave agents are duplicated on every Access Points are being dispatched to the every connect client system to the APs. When the duplicated salve agent at the client system detects any new Access Point, it automatically builds and sends an information packet INFO (SSID, MAC-Address, Vendors Name, Channel Used) of the Unauthorized AP to Duplicate Agent to the connected AP. The Slave Agent at AP transmits this Information to its Master Agent on the Server. At the server the details of the suspected AP are detected and matched with that of the information stored into the repository about all the access points.

If the information is matched and the AP is found ratified then a new slave agent is generated and send to that AP, rather if it's spotted as a client MAC address, a disassociation frame is send to all APs to inform them not to connect with it, else if the particulars doesn't match with the either of it then the MAC-Address of the AP is fetched from the INFO, the port at which the MAC-Address is coupled is examined and then be blocked for any LAN traffic Figure 4 will illustrate the system architecture of WLAN Multi-agent sourcing methodology.

This would then habitually deactivate the RAP from executing any network activity on the Wireless Network. And also prevent the clients (if any) connected to the AP by giving up the connection and get associated to the nearest AP which is certified. This is a very simple and most adequate method for completely routing out the Rogue Access Points from the network. [4][7]

This Methodology has the following owing stuffs:

It doesn't require any specialized hardware;

The proposed algorithm discovers and entirely eliminates the RAPs from network;

It provides a cost-effective result;

Due to multiple master agent's possibility of network congestion or delays is reduced.

The proposed technique can block RAPs as well as eradicate them from the networks both in form of Unauthorized APs or as a Rogue Clients Acting as APs.

Clear and easy to implement algorithm makes this architecture robust.

Proposed technique is very reliable and cost effective, as it deals with manifold level of detection and doesn't require any specialized hardware device

c.c. Rogue Access Point Detection and Prevention Techniques in W-LAN

"Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN" about different RAP detection techniques with their pros and cons [7]. This paper contains techniques,

RAP Detection Scheme Using Statistical Techniques. Goal of this method is to detect evil twin attacks in real time under real wireless network environments. The method presents two algorithms to detect evil twin attacks: Trained Mean Matching (TMM) and Hop Differentiating Technique (HDT).

Detection of Rogue Access Point using Timing based Scheme. This method considers a scenario when a wireless station tries to join a WLAN to access the Internet.

Detection of RAP using Received Signal Strengths. This method proposes a novel fake AP detection method in the client-side.

A Novel Approach for RAP detection on Client Side. This method identifies existing rogue access point detection methods. This Study shows techniques that collect constructive or precise information from network to determine whether a device is rogue or not.

Talking about pros and cons of this system Pros will be, it can detect Man in the middle and evil twin attack efficiently, there is no need to modify network architecture if you are using this method, as it works on client side, Any Client side device can serve as detection mechanism, no special device needed for detection and cons this method only notify user about rogue access point.

Monitoring Systems

d.a. MAP: A Scalable Monitoring System for Dependable 802.11 Wireless network

The MAP project, which includes a scalable 802.11 measurement system that can provide continuous monitoring of wireless traffic to quickly identify threats and attacks. The MAP project, which includes

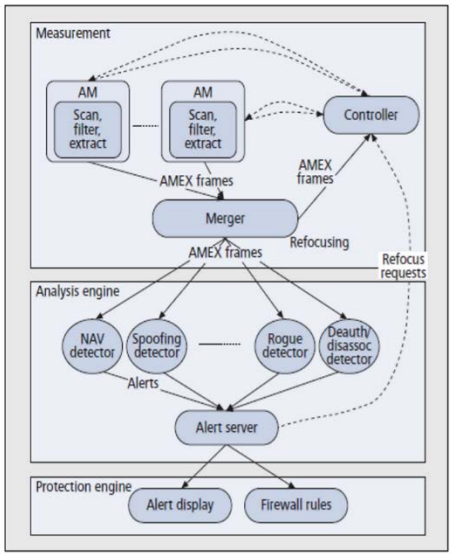

Figure 5: The Map architecture: dashed lines are controlled streams and bold lines represent Data.
Source: Map: a scalable monitoring system for Dependable 802.11wireless Research Paper.

That can provide continuous monitoring of wireless traffic to quickly identify threats and attacks. The MAP system makes several contributions: novel channel-sampling strategies, a flexible mechanism for "refocusing" the attention of the measurement system to address changing needs of the analysis modules, a plug-in architecture for analysis components, and a range of attack detectors but coordinated sampling reduced frame-capture redundancy, refocusing was able to improve the effectiveness of our attack detectors, and performance was reasonable at the scale of a modest building. [8] Figure 5 illustrate the MAP Architecture.

b. Tracking

e.a. Tracking Mobile Users in Wireless Networks via Semi-Supervised Co-Localization

This research focuses on Tracking Mobile Users in Wireless Networks. Locating large quantities of users in a wireless network is an important task. To solve this problem this research developed a novel machine-learning-based approach that combines collaborative filtering with graph-based semi supervised learning to learn both mobile-users' locations and the locations of access points. This framework exploits both labeled and unlabeled data from mobile devices and access points. Simultaneously recovering the locations of both mobile devices and access points, this is call colocalization, using labeled and unlabeled RSS (received-signal-strength) data from both mobile devices and access points. This research uses two-phase solution. First build a manifold-based model from a batch of labeled and unlabeled data in an offline training phase and then use a weighted nearest-neighbor method to localize a mobile client in an online localization phase. Then extend the two-phase co-localization to an online and incremental model that can deal with labeled and unlabeled data that come sequentially and adapt to environmental changes. Finally embed an action model to the framework such that additional kinds of sensor signals can be utilized to further boost the performance of mobile tracking.

II. Solution

Most common problem of wireless network is the unauthorized access by the unauthorized intruders in current era. Different intruders trying to access to private networks using various methods. Therefor wireless network should have vast area of knowledge about the intruders, most of the Wireless Local Area Network (W-LAN) used the manual system for detect or prevent the intruders as an example when intruder trying to access a W-LAN, W-LAN security system detects intruders using their network policies and prevent them. Some other W-LAN security systems, they detect the unauthorized access and keep letting access the W-LAN. They do not take the actions to prevent the intrudes.

This research trying to provide most securable environment for wireless networks. Research include mainly intruders detect, prevent and track them in most securable way. Firstly, identifying "who are the unauthorized accesses and are they really harmful to the wireless network". Then check intruder's violation history using particular technics include in system.

To check the intruder's history, wireless network security system has special network called Wireless WAN, which is connected together all the wireless LAN around the world. All the wireless-LAN has connected to wireless-WAN, if any violation within the particular Wireless-LAN, it alerts to Wireless WAN. Wireless-WAN has special database which is included all the details about the intruders who had already done the violations before. With compare ring historic detail about the intruders, determine the intruder's situation. If the intruder cannot find in the Wireless-WAN, that intruder automatically added to the database with all the information about the intruder.

To detect the intrudes in this research used both traditional and newly introducing methods. Traditional way of detect the intruders is when anyone who trying to access the wireless network, determine whether if they are authorized or not using wireless network policies. Newly introducing method uses wireless network traffic and analyze traffic using particular algorithm to detect unauthorized access.

Wireless network security system uses an algorithm to analyze the users in the network background.

Algorithm analyze periodically traffic of the wireless network and keep the record of every periodic records. Algorithm continuously analyze wireless network periodically. If the algorithm detects any abnormal behavior within the network, wireless network security system keeps an eyes on about particular user. Anyhow particular time period record mismatch with previous records, Wireless-LAN suddenly identify there are something wrong with the Wireless-LAN and then check any violation occurs to the system using Wireless-LAN policies.

a. Analyze network traffic

As indicate above, using specific algorithm analyze the traffic of the W-LAN periodically to get the all the information about the W-LAN users. Mainly use the devices mac address to identify the users separately. Here monitor the both register uses of the W-LAN and unauthorized users. Register users monitored because, if they are trying to access the resources which are not

allocated to them and then analyze the which part of the W-LAN they are trying to access mostly then identify and give higher security to those part of the W-LAN. And also monitor the unauthorized access from outside the WLAN. This help system to detect and prevent the hackers before the attacking W-LAN.W-LAN algorithm also provide the proper knowledge about which time period hackers can attack the W-LAN and what part of the W-LAN mainly aim to attack.

b. W-WAN Database

Thousands of W-LAN spreads around the world and single W-LAN hard to protect from hackers, for that reason this research provide proper technics to combine them together for more secure. All the WLAN has common database which has connected to W-WAN. That database has most of the detail about the hackers who are trying to attack the W-LAN. When unauthorized access occurs to W-LAN, WLAN can check the device detail using W-WAN database and check violation history about device. If W-WAN database does not have the detail about that particular device-WAN database can update the new detail about device.

III. Conclusion

Wireless networking provides numerous opportunities to increase productivity and cost cutting it is also changing an organization's whole computer security risk profile. Although it is difficult to totally eliminate all risks related with wireless networking, it is possible to achieve a practical level of overall security by implementing a systematic approach to accessing and managing risks.

The research paper has stated new methodology for eliminating and detecting intruders. For the detecting it has used some traditional and new methods. The new method is to analyses the intruders by use of an algorithm and to analyses the pattern intruders that going to effect the network by using the algorithm. The algorithm will identify the time period of the intruder attacks. Using this network can be protected from the intruders automatically. Finally, the information about the intruder will automatically save with in the syslog and it'll block the intruder from the next attack.

IV. Future Work

In futre work there can be several things to develop with time. This research paper used the particular algorithm to detect and prevent the intruders.in future, that algorithm can be develop to be most intelligently using artificial intelligent. And also get all the hackers detail around the world using some richest technology. Since then can find out every hacker's violation history with his personal details. Using those details W-WAN can provide more accurate detail about the hackers.

References

[1] Gerkis," A Survey of Wireless Mesh Networking Security Technology and Threats", SANS Institute 2000 – 2005, September, 2006, [online] Available: https://www.sans.org/readingroom/whitepapers/networkdevs/survey-wirelessmesh-networking-security-technology-threats-1657 [Accessed: 25-Feb- 2016]

[2] A.Singh, A.Vaish and P.K.Keserwani, "Research Issues and Challenges of Wireless Networks", 2014IJARCSSE, February 2014, [online] Available http://www.ijarcsse.com/2_February2014/V4I20175.pdf [Accessed: 15-feb-2016]

[3] P.A. Ochang and P.Irving, "Performance Analysisof Wireless Network Throughput and Security Protocol Integration", International Journal of Future Generation Communication and Networking, January 2016, [online] Available http://www.sersc.org/journals/IJFGCN/7.pdf [Accessed 12-feb-2016]

[4] S.Sang et al. "Dynamic Access Control Model for Security Client Service in Smart Grid", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, June 2014, [Online] Available http://www.hindawi.com/journals/ijdsn/2014/181760/ [Accessed 12-Feb-2016]

[5] P.G.Sasane and S. K. Pathan, "Detection and Elimination of Fake Access Points in WLAN using Multi Agents and Clock Skew Methodology", International Journal of Engineering Research & Technology, june-2014, [online] Available http://www.ijert.org/view-pdf/10062/detection-andelimination-of-fake-access-points-in-wlan-usingmulti-agents-and-clock-skew-methodology [Accessed 8-feb-2016]

[6] S.Gambhir et al., "A Survey onRouting Protocols andVulnerabilitiesinMobile Ad-Hoc Network (MANETs)", JRASET2015,December2015,[online]https://www.researchgate.net/publication/286931284_A_Survey_on_Routing_Protocols_and_Vulnerabilities_in_Mobile_Ad-Hoc_Network_MANET s [Accessed 21-feb-2016]

[7] Sachin et al.,"Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN ", International Journal of Advanced Research in Computer Science and Software Engineering, octomber2013, [online] Available http://www.ijarcsse.com/10_October2013/V3I10-0419. Pdf [Accessed 20-feb-2016]

[8] Y.Sheng et al., "Map: a scalable monitoring system for dependable 802.11 wireless networks", IEEE Wireless Communications,October2008,[Online]Availablehttp://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=465312 7 [Accessed 6-feb-2016]

[9] J.J.Pan et al., "Tracking Mobile Users in Wireless Networks via Semi-Supervised Co-Localization", IEEE, January 2015, [online] Available http://www.cs.ust.hk/~qyang/Docs/2011/TPAMI 2010-10-0806.pd f [Accessed 24-feb-2016]

Authors

First Author – K.A.L.K.Dhananjaya Arachchi, Under Graduate (BSc IT), Sri lanka Institute of Information Technology(Pvt) Ltd, lahirukdhananjaya@gmail.com.
Second Author – K.A.D.K.N.Peiris, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, kavindika@gmail.com.
Third Author – M.Nishanthan, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, n.m.nishanthan@gmail.com.
Forth Author – I.D.M.D.Sandimali, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, dsiidamgedara@gmail.com.
Fifth Author – R.Indrakumar, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, indran311@gmail.com.
Sixth Author – W.A.L.K.Athukorala, Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, kanchanaathukorala123@gmail.com.

Seventh Author – U.G.P.R.Weeragoda , Under Graduate (BSc IT), Sri Lanka Institute of Information Technology(Pvt) Ltd, prathibha0303@gmail.com.
Eighth Author – Dhishan Dhammearatchi, Lecturer(Bsc Hons(UK), MSc (UK), CCNP, MCSSL(SL), MBCS(UK), MIEEE, TM (CC), MCKC (SL)), Sri Lanka Institute of Information Technology(Pvt) Ltd, dhishan.d@sliit.lk.

Correspondence Author – – K.A.L.K.Dhananjaya Arachchi, lahirukdhananjaya@gmail.com, +94714113696