J. Res. Technol. Eng. 5 (1) , 2024, 08-12

Journal Of Research Technology & Engineering
www.jrte.org

Improved Digital Security Applications for Smart Card

* Aseel nadhum kadhum

College of Imam AL Kadhim (AS) Islamic Sciences // Babylon Branch, Iraq

*Easeel18@yahoo.com

Received:11 Dec 2023; Revised: 18 Dec 2023; Accepted: 27 Dec 2023; Available online: 10 Jan 2024

Abstract: With the rapid expansion of wireless networks and mobile computing applications, the quality of service (QoS) of mobile ad hoc networks (MANETs) has received increasing attention. Security is an important aspect of providing QoS in a MANET environment. Without the protection of a security mechanism, attacks on a QoS distortion system can lead to poor QoS performance, interference of resource consumption, or even failure of QoS provisioning. Due to the characteristics of MANET, such as diversity of static topology and limited computational and communication power, traditional security measures cannot be used, and new security technologies are inevitable. However, little research has been done on this topic. This article discusses security issues of MANET systems and QoS. Therefore, this research works to develop methods to evaluate the security design review periodically to ensure that all vulnerabilities such as security vulnerabilities have been discovered and corrected and their discovery and correction explained. Analyze and determine the basic security and protection requirements in the system to be designed. Design a network model using GloMoSim, determine node locations, communication characteristics, technology used, and identify potential weak points in the model that represent a security threat.

.

Index Terms: Security, Networking, IEEE, Bluetooth, AODV.

1 INTRODUCTION

In remote systems computers are connected and talk to each other via a marked electromagnetic dynamic flow around, the more commonly used transmission is the radio waves.
Remote transport uses the microwave spectra: the accessible frequency response arranged around 2.4 GHz ISM (Industrial, Scientific and Medical) band for data transfer capacity of around 83 MHz, and around the 5 GHz U-NII (Unlicensed-National Information Infrastructure) band for a transfer speed of around 300 MHz partitioned into two sections. The correct recurrence assignments are set by laws in the diverse nations, similar laws additionally direct the most extreme dispensed transmission force, area (indoor, open air). Such a remote radio station system has a scope of around 10-100 meters to Km, contingent upon the emanation control, the information, the recurrence, and the sort of receiving wire utilized. A wide range of models of reception apparatus can be utilized: Omnis (omnidirectional radio wires), division receiving wires (directional reception apparatuses), explanatory plates, or Waveguide guides [1].
The other day kind of transit bolster is this infrared: Infrared beams can't enter misty The material has a littler of around 10 metres. For those purposes, infaraed innovation is to on the most part utilized for little gadgets in WPANs (Wireless Personal Area Networks), for example to associate a PDA to a tablet in the room [1].
The major contributions of this research are:
(a) Design of security display in which the information parcels are encoded and unscrambled utilizing various calculations where the choice plan is arbitrary.

(b) Design of a security system to counteract and identify attacks on the QoS.

2 Standards

There by and by three primary gauges to remote systems: the IEEE 802.11 family, Hiper LAN, and, Bluetooth [2].

2.1 IEEE 802.22 FAMILY

IEEE 802.11 is a standard issued by the IEEE (Institute of Electrical and Electronics Engineers). From the motivation behind the physical layer, it describes three non-interoperable procedures: IEEE802.11 FHSS (Frequency Hopping Spread Spectrum) and IEEE 802.11 DSSS (Direct Sequence Spread Spectrum), which uses both the radio average at 2.4 GHz, and IEEE 802.22 IR (InfraRed). An expert data average is 1-2 Mbps. that is specific for delivered a gathering of various measures:

IEEE 802.11a (advertised at Wi-Fi) works at 5 GHz U-NII strap utilizing OFDM (Orthogonal Frequency Division Multiplexing) transportation procedure, and hold a most extreme information average of Mbps. IEEE 802.11a is contradictory with 802.11b, in light of the fact that utilize distinctive frequencies [2].

IEEE 802.11b (advertised Wi-Fi), works at 2.4 GHz ISM band. Information average is 1,2,5 or 11 Mbps, naturally balanced relying upon flag quality. The transportation go relies upon the information rate, differing to 50 meters indoor (200 meters outside) from 11 Mbps, to 150 meters indoor (500 meters' open air) for 1 Mbps, the transportation rang at likewise corresponding as the flag control[2].

I EEE 802.11g: at the 2.4 GHz band and hold an information average of up to 20 Mbps. It utilizes together OFDM and DSSS to guarantee similarity for IEEE 802.11b standard.

IEEE 802.16 (showcased as WiMAX), it intended at WMANs (Wireless Metropolitan Area Networks) also along these lines for defeat the range confinements of IEEE 802.11. It works in frequencies run from 10 to 66 GHz, and ought to guarantee organize scope for a few square kilometers. at the IEEE 802.16 standard, IEEE 802.16a was determined, which works at 2-11 GHz band know and unravels the line – of sight issues getting to utilizing the 10-66 GHz band [3].

Channel get to procedure: A pivotal mark in conduit get for systems to remote systems is that it isn't conceivable for transmit and to detect a transporter for parcel crashes in the meantime. In this way nothing real road to execute a CSMA/CD (Carrier Sense Multiple Access/Collision Detection) convention, for example, in wired Ethernet [3].

IEEE 802.11 used a channel get for designing of sort CSMA/CA, which is intended to implement collision evasion (or possibly to attempt). The CSMA/CA convention expresses it's a hub, after detecting that channel is occupied, should sit tight for a between the frame dividing before endeavoring to transmit, at that point pick an irregular postponement relying upon the Competition window. The package collection is recognized by the collector to the transmitter. If the transmitter does not get the affirmation bundle, it sits tight for a deferral as indicated by the paired an exponential decline calculation, that expresses estimate is multiplied at each attempt. Unicast information parcels are utilizing a more solid component. The Source Movements a RTS (Request to Send) bundle to goal, where answers at (parcel to collect) parcel upon gathering. In the event that the exporter effectively gets the CTS, it sends the information parcel [4].

2.2 HiperLAN

HiperLAN 1 utilizes the 5 GHz band and offers an information rate of 10 - 20 Mbps. HiperLAN 2 utilizes the 5 MHz band and offers an information rate up to 54 Mbps. A standard-related it HiperLAN, opponent of IEEE 802.16 while went for giving range scope. It works in the 2-11 GHz band [5].

2.3 Bluetooth

Bluetooth is standard composed by a group of privately owned businesses, for example, Agere, Ericsson. IBM, Intel, Microsoft, Motorola, Nokia and Toshiba. Bluetooth works in the 2.4 GHz band utilizing FHSS and it has a short scope of activity of around 10 meters. to such qualities minimal effort, Bluetooth suitable for little WPANS and is likewise utilized for associate Extensions, for example, consoles, printers, or cell phone headsets. Bluetooth radio innovation works in the Bluetooth. Reporter are sorted out in little systems called piconets, each piconet being made out of an ace and 1-7 dynamic slaves. Different piconets can cover to shape a scatter net [6].

3 SYSTEM DESIGN

Designing a system for selecting QoS options requires a set of basic steps. Below is a detailed breakdown of the security system design for this purpose [7] [8]:
1. Analysis: Analysis of potential scenarios and threats that may threaten the quality of service. Searching for weak points in the system and points from which one can judge.
2. Apply all of the above: Modern protection such as firewalls and detection systems must be adhered to protect network privacy and prevent high-quality service encryption.
3. Security Management: Within the careful design of the system, there must be a security management feature, as a strong VPN for any reason can affect the quality of service.
4. Monitoring: Completely monitor the network and systems for early detection of any suspicious activity that may affect the quality of service and rapid response to such actions.
5. Proper evaluation to ensure: After careful design of the system, it is necessary to conduct a physical evaluation to ensure its full effectiveness against innovations.
6. Staff training: Conduct personal training on how to deal with situations, coordinate service quality, and respond to different situations.

Designing a real security system requires consideration of various aspects of security, personal data protection, and personal data monitoring.

4 PERFORMANCE EVALUATION

The accompanying measurements were utilized to assess the execution of the information and defeat security. The accompanying measurements are assessed the productivity notwithstanding the adequacy of the conventions [9].

- Average performance in the context of security system design refers to the efficiency of routing and managing information packets transmitted between specific sources and specific targets. If the proportion of information packages transmitted between sources and recipients is high compared to information packages initiated by sources, this reflects high efficiency in direction and management. Overall, this procedure demonstrates the effectiveness and efficiency of the design and implementation of the comprehensive security system in achieving its objectives effectively and accurately [10].
- Packet throughput ratio measures the efficiency of transporting packets from sources to recipients compared to the packets expected to be transported based on the overall design of the security system. If the percentage is high, this indicates high efficiency in the process of sending packets and thus indicates good efficiency in the overall design of the security system. Through this procedure, supervisors and security managers can accurately evaluate the efficiency of this process and improve it if necessary [11].
- End-to-end delay refers to the total time required for the message to be received from the original source until it reaches its intended destination in the system. In other words, it measures the total time couriers need from transmitting from the source to receiving at the destination. This time includes all possible delays for all parties involved in the transfer process, and this concept represents an important aspect in measuring the efficiency of the transfer process and ensuring that the system is able to achieve outstanding performance during the time period. Suitable [12].

5 SIMULATION RESULTS

Figure 1 indicates that the implementation of information security can affect various values obtained using GloMoSim. Locking can result in varying data, varying speeds, and a varying number of axes. Figure 1 shows the relationship of average start-to-end delay versus the number of nodes. It reflects how the security process affects the response time, speed and efficiency of the network with GloMoSim.

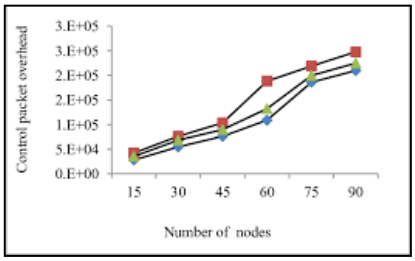

Fig.1. Number of Control Packets Vs Number of Nodes

The Fig.2 shows an examination of public expenditure monitoring and its relationship to the number of axes at different speeds and the detection and monitoring of loopholes in the system. He also points out that increases in control public spending can be expanded by backing out of the cycle, and it is clear from the Fig.2 that multi-speed center expansion leads to a small proportional increase in control public spending, and this can mainly be attributed to continuing disappointments, Naturally, to the increasing brutality. These studies can be used to improve security and monitoring policies within government systems and companies to ensure that there are no abuses or violations of certain policies and procedures.

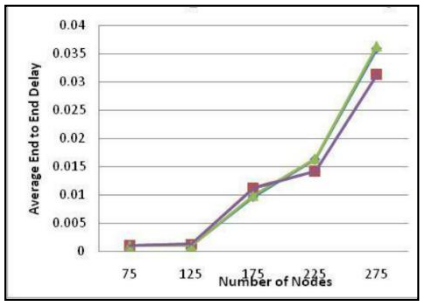

Fig.2. Average End-to-End Delay Vs Number of Nodes

6 THE LIMITATION

The attacker was able to access all sent paths. If these constraints are met, the probability of reconstruction will be low in the area of information security of the smart card. This includes the inability to improve security and enhance protection against attackers who may attempt to access transmitted paths.

To ensure security in future studies, it is necessary to ensure that the highest standards of smart card security and data protection are met. You can check with your card provider to ensure that any necessary restrictions and procedures are implemented correctly. It is also best to review globally accepted security guidelines and specifications, such as PCI DSS standards, and ensure that the private system infrastructure provides adequate protection for the data being transmitted.

8 CONCLUSION

The research aims to improve information security on mobile devices using a new strategy that uses unsystematic selection of cryptographic accounts on GloMoSim. The results were compared between the implementation of the information security agreement and the training course with and without the use of encryption. The results showed a significant increase in data transfer rate of up to 80% compared to unencrypted data. The research encourages verification of secure course disclosure to protect against security risks and dark vulnerability attacks.

From a security perspective, this research is important because it investigates new strategies to improve information security, and also seeks to encourage the dissemination of secure course verification. Technically, the research focuses on providing information security and improving the functionality of stacked systems in a robust and highly portable manner.

REFERENCES

[1] Umar, A., Mayes, K., & Markantonakis, K. (2015, February). Performance variation in host-based card emulation compared to a hardware security element. In *2015 First Conference on Mobile and Secure Services (MOBISECSERV)* (pp. 1-6). IEEE.

[2] Kaur, J., Kumar, A., & Bansal, M. (2017, September). Lightweight cipher algorithms for smart cards security: A survey and open challenges. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 541-546). IEEE.

[3] Li, W., & Song, H. (2015). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE transactions on intelligent transportation systems*, *17*(4), 960-969.

[4] Shuyao Yu, Youkun Zhang, Chuck Song and Kai, Chen,"A security architecture for Mobile Ad Hoc Networks ", Proc.

[5] Azees, M., Vijayakumar, P., & Jegatha Deborah, L. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems*, *10*(6), 379-388.

[6] Winkler, T., & Rinner, B. (2014). Security and privacy protection in visual sensor networks: A survey. *ACM Computing Surveys (CSUR)*, *47*(1), 1-42.

[7] Engoulou, R. G., Bellaïche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. *Computer Communications*, *44*, 1-13.

[8] Bariah, L., Shehada, D., Salahat, E., & Yeun, C. Y. (2015, September). Recent advances in VANET security: a survey. In *2015 IEEE 82nd vehicular technology conference (VTC2015-fall)* (pp. 1-7). IEEE.

[9] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications*, *37*, 380-392.

[10] Saini, M., Alelaiwi, A., & Saddik, A. E. (2015). How close are we to realizing a pragmatic VANET solution? A meta-survey. *ACM Computing Surveys (CSUR)*, *48*(2), 1-40.

[11] Bariah, L., Shehada, D., Salahat, E., & Yeun, C. Y. (2015, September). Recent advances in VANET security: a survey. In *2015 IEEE 82nd vehicular technology conference (VTC2015-fall)* (pp. 1-7). IEEE.

[12] Rehman, S. U., Khan, M., Zia, T., & Zheng, L. (2013). Vehicular ad-hoc networks (VANETs): an overview and challenges. *Journal of Wireless Networking and communications*, *3*(3), 29-38.