International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

EAACK: A Secure Intrusion Detection System for MANETs

Prasad Barde*, Deven Agrawal, Sakshi Agrawal, Sampada Diwan and Prof. Swati Salunkhe

Department of Computer engineering Jayawantrao Sawant college of Engineering Pune, India

Received 25 April 2023, Accepted 16 May 2023, Available online 18 May 2023, **Vol.13, No.3 (May/June 2023)**

Abstract

Mobile Ad-hoc Networks (MANETs) are becoming increasingly popular due to their ability to provide communication in areas where infrastructure is not available. However, the lack of a centralized infrastructure also makes them vulnerable to security threats such as intrusion attacks. In this paper, we propose a secure intrusion detection system called EAACK (Enhancing Acknowledgment- based Intrusion Detection System) for MANETs.

Keywords: *Mobile Ad-hoc Networks, Centralized infrastructure etc.*

Introduction

Because of their natural mobility and scalability, wireless networks are always desired due to the fact that the primary day of their invention. As a result of the improved technology and decreased prices, wi-fi Networks have gained much more preferences over stressed networks in the past few decades. By means of definition, cellular advert hoc community (MANET) is a set of cell nodes Prepared with both a wireless transmitter and a receiver that speak with every other via Bidirectional wi-fi links both immediately or indirectly. Commercial remote gets right of entry to and control through Wi-fi networks are becoming increasingly more famous these days. One of the main Benefits of wi-fi networks is its ability to permit data verbal exchange between exclusive parties and nonetheless preserve their mobility but, this communique is confined to the range of Transmitters. This means that nodes cannot speak with each other while the gap Among the 2 nodes is past the communique range of their own. MANET solves this Trouble by using allowing intermediate events to relay facts transmissions.

Background

MANETs are composed of mobile nodes that communicate with each other without the need for a centralized infrastructure. This makes them useful for a variety of applications such as military operations, disaster response, and transportation. However, the lack of a centralized infrastructure also makes them vulnerable to security threats such as intrusion attacks.

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.13.3.6

As discussed earlier than, due to the limitations of most MANET routing protocols, nodes in MANETs count on that other nodes always cooperate with each different to relay statistics. This Assumption leaves the attackers with the possibilities to reap sizable impact at the network with simply one or two compromised nodes. To deal with this trouble, an IDS must be brought to decorate the safety level of MANETs. If MANET can stumble on the attackers as quickly as they input the network, we will be able to completely dispose of the potential damages because of compromised nodes at the primary time. IDSs typically act as the second layer in MANETs, and that they are a brilliant supplement to existing proactive tactics.

Anantvalee and Wu presented a completely thorough survey on modern IDSs in MANETs. In this phase, we especially describe three existing approaches namely Watchdog, TWOACK, and Adaptive ACKnowologement (AACK).

Literature Survey

1. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

In this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. They first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then they discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally

they survey the current security solutions for the mobile ad hoc network.

2. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23

An ad hoc network is a group of wireless mobile computers (or nodes), in which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. In this paper, we present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne.

Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of- Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives.

Methods

In EAACK, each node in the network is assigned a unique digital signature and authentication key. When a node sends a message, it attaches its digital signature and authentication key to the message. The receiving node then verifies the digital signature and authentication key to ensure that the message is coming from a legitimate source. If the verification fails, the receiving node sends an alarm to the other nodes in the network.

Algorithm

DSA and RSA

We witness that DSA scheme always produces slightly less network overhead than RSA does. This is easy to understand because as the signature size of DSA is much smaller than the signature size of RSA. However, it is interesting to observe that the RO differences between RSA and DSA scheme varies with different number of malicious nodes. The more malicious nodes there are the more routing overhead RSA scheme produces. We assume this is due to the fact that more malicious nodes require more acknowledgement packets, and thus increases the ratio of digital signature in the whole network overhead.

With respect to this, we find DSA a more desirable digital signature scheme in MANETs. The reason being data transmission in MANETs consumes the most battery power. Although DSA scheme requires more computational power to verify than RSA, considering the tradeoff between battery power and performance, DSA is still preferable.

Comparison of DSS and RSA

- DSS provides us digital signatures. But it does not provide us key exchange and encryption. RSA provides us digital signatures, encryption and key exchange.
- DSS and RSA both are based on public key technique.

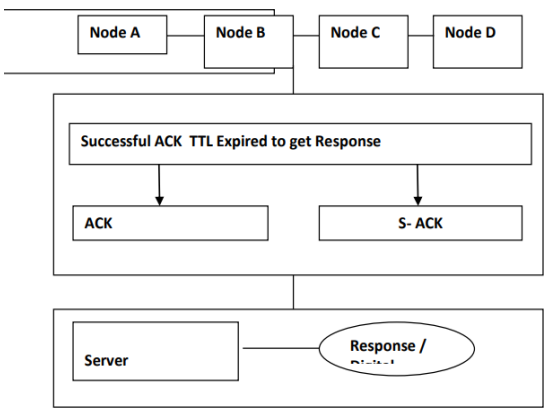
The Direct Digital Signature

- Understanding a direct digital signature starts by analyzing there are only two parties involved in the passing of the signed information: the sender and the receiver. Direct digital signatures only require these two entities because the receiver of the data (digital signature) knows the public key used by sender. And the sender of the signature trust the receiver not to change the document anyhow.

The Arbitrated Digital Signature

- Implementing an arbitrated digital signature invites a third party into the process that called a "trusted arbiter." The role of this trusted arbiter is usually twofold: initially this independent third party check the probity of the signed message. then, the trusted arbiter dates, or time-stamps, the document, verifying receipt and the passing on of the signed document to its intended final destination.

System Architecture



Expected Result

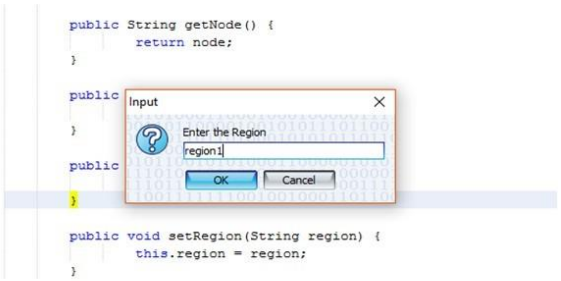
EAACK a secure intrusion detection system for manets is aimed at providing a secure solution for the detection of malicious activities in Mobile Ad-hoc Networks (MANETs). This project is expected to provide an efficient and reliable mechanism to detect intrusions and unauthorized access attempts in MANETs. The results of this project are expected to be a comprehensive system that can detect malicious activities in MANETs, including malicious nodes, packet drops, and other attacks. The system should also be able to identify false positives and false negatives while providing real-time alerts and notifications. The

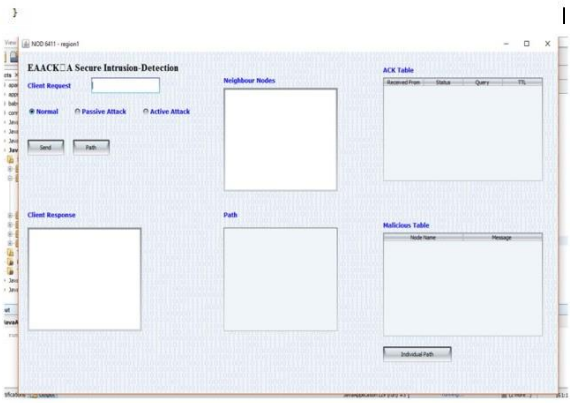
system should also be able to generate reports based on the analysis of the collected data.

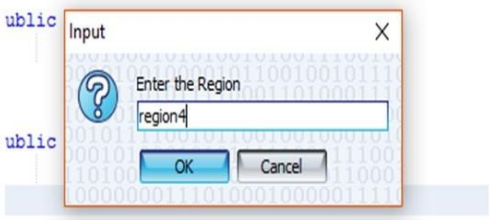
It will also provide an efficient way to detect and respond to malicious activities in real-time. In addition, it will also be able to identify potential vulnerabilities in the network and recommend countermeasures.

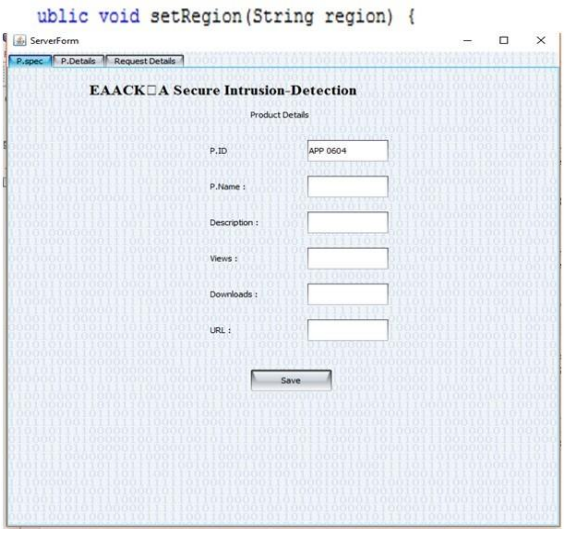
Furthermore, the project is expected to provide insights into how EAACK can be used for better security solutions for MANETs.

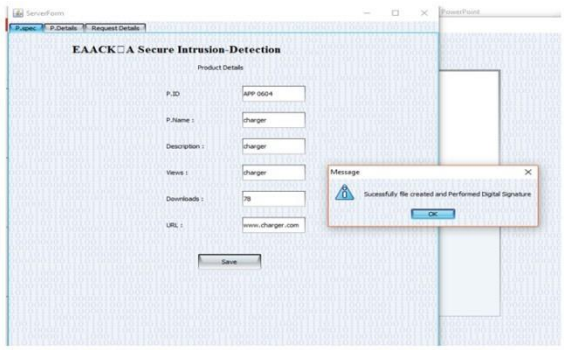
- **Screenshots of Implementation Step by Step**

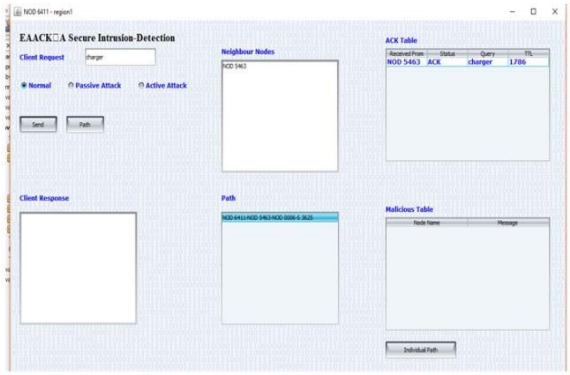


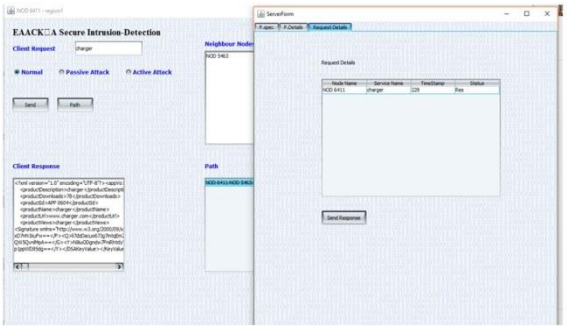


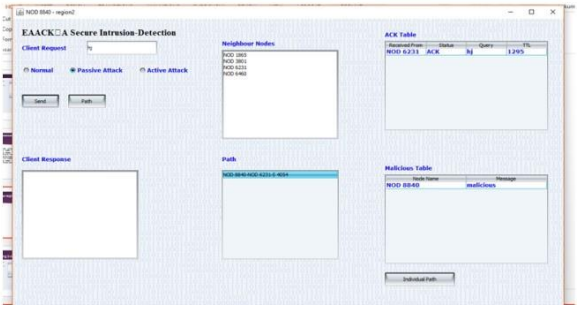


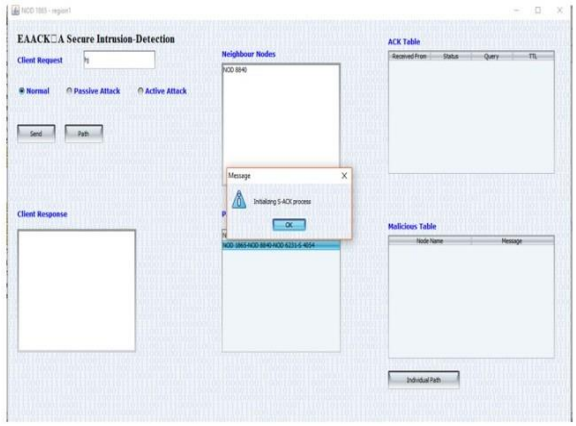


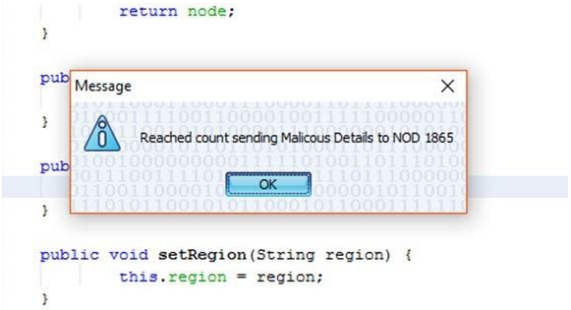


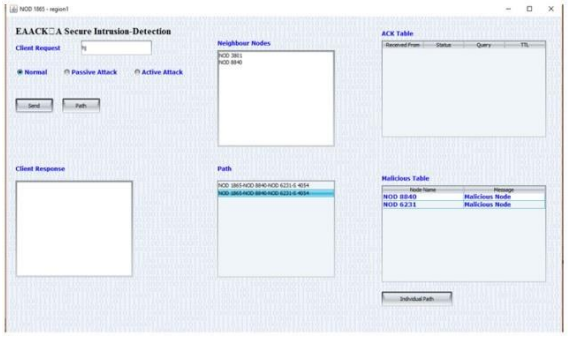


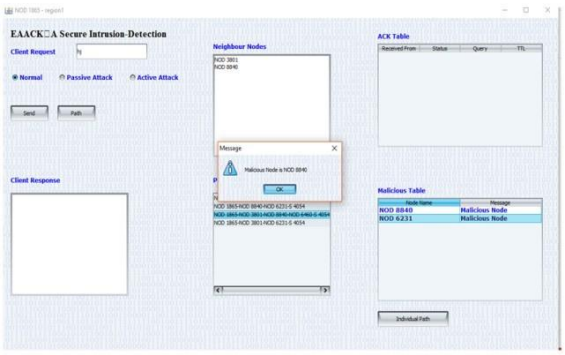












Conclusion & Future Work

In this paper, we proposed a secure intrusion detection system called EAACK for MANETs. The system is based on the acknowledgement-based intrusion detection (ABID) method and enhances it by incorporating techniques such as digital signature and authentication. The simulation results showed that EAACK was able to detect and respond to intrusion attempts with high accuracy and low false alarm rate.

References

[1] S. R. Das, C. E. Perkins, and E. M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," IEEE Personal Communications, vol. 8, no. 1, pp. 16– 28, 2001.

[2] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," IEEE INFOCOM, vol. 3, pp. 1567– 1576, 1998.

[3] S. R. Das, C. E. Perkins, and E. M. Royer, "A secure routing protocol for ad hoc networks," IEEE Personal Communications, vol. 7, no. 5, pp. 28–34, 2000.

[4] T. Anantvalee and J. Wu. A Survey on Intrusion Detection in Mobile Ad hoc Networks. In Wireless/Mobile Security, Springer, 2008.

[5] L. Buttyan and J.P. Hubaux. Security and Cooperation in Wireless Networks. Cambridge University Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, L. Benini, "Modeling and Optimization of a Solar Energy Harvester System for Self- Powered Wireless Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 7, pp. 2759-2766, July 2008.

[7] V. C. Gungor, G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approac," IEEE Trans. on Industrial Electronics, vol. 56, no. 10, pp. 4258-4265, Oct 2009.

[8] Y. Hu, D. Johnson and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In the Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-13, 2002.

[9] Y. Hu, A. Perrig, and D. Johnson. ARIADNE: A Secure On-Demand Routing Protocol for Ad hoc Networks. In the Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23, Atlanta, GA, 2002.

[10] G. Jayakumar and G. Gopinath. Ad Hoc Mobile Wireless Networks Routing Protocol – A Review. In Journal of Computer Science 3(8): 574-582, 2007.

[11] D. Johnson and D. Maltz. Dynamic Source Routing in Ad hoc Wireless Networks. Mobile Computing, Kluwer Academic Publishers, Chapter 5, pp. 153-181, 1996.

[12] N. Kang, E. Shakshuki andT. Sheltami. Detecting Misbehaving Nodes in MANETs. The 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), ACM, pp. 216-222, November, 8-10, Paris, France, 2010.

[13] N. Kang, E. Shakshuki andT. Sheltami. Detecting Forged Acknowledgements in MANETs. The 25th International Conference on Advanced Information Networking and Applications (AINA), IEEE Computer Society, Biopolis, Singapore, March 22-25, 2011.

[14] K. Kuladinith, A.s Timm-Giel and C. Görg. Mobile Ad-Hoc Communications in AEC industry. In Journal of Information Technology in Construction Vol. 9, pp. 313-323, 2004.