Efficacious Framework for The Detection of Link Flooding Attack in Mobile Ad Hoc Network

M. Gautham [1], D. Chitra [*2], B. Samitha [3]

[1] Assistant Professor, Department of ECE, Mahendra Engineering College, Namakkal, Tamil Nadu, India
[2] Professor, Department of ECE, Mahendra Engineering College, Namakkal, Tamil Nadu, India
[3] PG Scholar, Department of ECE, Mahendra Engineering College, Namakkal, Tamil Nadu, India
Emails: gauthamm@mahendra.info; chitravalli2000@gmail.com

Abstract

A novel honey pot deception trace back model, or honey pot IDS, is offered. The system is located on the server, which is the site of network intrusion deceptions. From there, it keeps an eye on all incoming traffic and uses nodes that carry out network weight age studies to continuously weigh the data. For every client connected to the server, it serves as a construct to look at the packet analysis and transmission path to which the IP processed the intrusion detection system. This LF-IDS detects intrusions using both anomaly-based and rule-based intrusion detection methods. By gathering and examining the packets from incoming traffic, the system initially collects data on the packet agent monitoring system. The trespasser is led to a honey pot that will be constructed as a mitigation site.

Keywords: MANET; LF-IDS; Link Flooding; Cluster head

1. Introduction

Advances in wireless communication technology have enabled mobile and ubiquitous computing, enabling "anywhere, anytime" communication services. Wireless ad hoc networking, an advanced technology, allows for out-of-range communication without a fixed backbone infrastructure support [1]. This allows for easy formation at any location, especially in areas where infrastructure-based systems are not feasible due to geographical or terrestrial constraints.

A wireless ad hoc network is a decentralized wireless network consisting of individual wireless hosts that can be quickly deployed in a specified area, creating a multi-hop packet radio network [2]. This decentralized design makes it more scalable than managed networks, making it suitable for applications where central nodes are not needed.

MANETs offer flexibility in communication but also pose significant research challenges, particularly in safety-critical applications. Due to their inherent characteristics, MANETs are highly vulnerable to security threats, including physical attacks, passive listening, and interference [3]. Without sufficient security, MNs can be easily taken over, impounded, and corrupted. Attackers can listen in on conversations, alter them, and even attempt to pass for another person.

Dynamic network topology can enable attackers to update routing information maliciously by pretending to have legitimate changes [4]. MANET nodes exchange information about network topology, allowing routes to be established. Intruders can give incorrect update information, leading to Denial of Service (DoS) attacks if spurious routing messages are propagated.

DOI: https://doi.org/10.54216/IJWAC.090105
Received: October 22, 2024 Revised: December 24, 2024 Accepted: January 21, 2025

MANETs' decentralized decision-making relies on cooperative participation among nodes, making it susceptible to attacks designed to eliminate this cooperativeness [5-6]. Malicious nodes can block or modify traffic, breaking the algorithm's cooperative nature. Traditional security mechanisms and key management schemes are not applicable due to the lack of existing infrastructure.

2. Related Work

Information security is crucial in computer networks and modern communication systems to protect against harm, theft, and attacks. Efficient security mechanisms should be well-designed, implemented, and employed [7-8]. Numerous methods and techniques have been developed to enhance security in wired and wireless networks. To provide sufficient security, desired properties must be achieved.

With symmetric key cryptography, a single, shared key is used by both the sender and the recipient of the communication to encrypt and decode it. Symmetric-key cryptosystems are faster and simpler than public-key cryptology, but their primary disadvantage is the need for a safe key exchange between the two unknown participants who are located far away [9]. Secret-key cryptography is another name for symmetric-key cryptography. The Data Encryption Standard (DES) is the most widely used symmetric-key scheme [10]. A cryptographic scheme known as public key cryptography [11] uses two keys: a private key for message decryption and a public key for message encryption. Only the recipient of the message is aware of the private or secret key; the public key is known to everybody.

The public key system involves the use of a public key to encrypt messages, while only the corresponding private key can decrypt them, making it nearly impossible to deduce the private key if the public key is known [12].

Public-key encryption is slower than symmetric key encryption, so a hashing function is created to produce a short fingerprint of a longer message, called a message digest [13]. Hashing functions can be keyed or non-keyed, compressing messages into digests (MIC) without using keys, or combining a message and a secret key to generate a message digest (MAC).

3. Proposed Methodology

The layer of mobile sinks, such as Personal Digital Assistants (PDAs), self-organize to form a mobile ad hoc network (MANET) with communication protocols applicable in a typical MANET. These devices collect data at a reduced energy cost near sensors and disseminate it, with a transmission range 5-20 times longer than a sensor node.

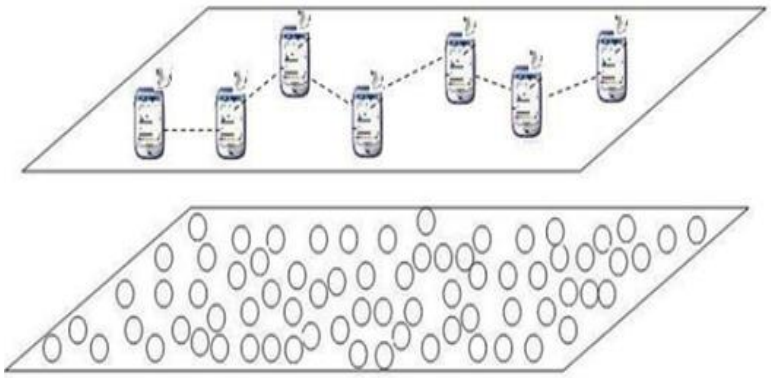

Figure 1: MSSSN Architecture

A mobile sink collects, processes, and shares data from its assigned region, handling localization, addressing, resource allocation, memory space, and time synchronization for sensor nodes. Its mobility in the sensor network field is facilitated through various techniques, from hand-carrying to automated vehicles.

A user sends a query to a mobile sink, which checks if it is the appropriate node to respond. If so, it collects data and responds to the user. If not, it broadcasts the query to all mobile sinks, similar to route

DOI: https://doi.org/10.54216/IJWAC.090105
Received: October 22, 2024 Revised: December 24, 2024 Accepted: January 21, 2025

discovery in MANETs. The appropriate node collects data from its assigned region and coordinates with other nodes, sending an appropriate reply.

4. Results and Discussion

Node capture attack poses a significant threat in Wireless Sensor Networks (WSN), as adversaries can physically capture SNs to compromise stored secret information. Random key pre-distribution schemes may compromise communication between non-captured nodes. In LEKM and IKDM, no communication between SNs exists, reducing key storage overhead and increasing network resilience against SN capture attack. Unique pairwise keys prevent SNs from compromising secure communication between non-compromised nodes.

LEKM pre-loads secret keys in CHs during network initialization, allowing adversaries to compromise stored keys once captured.

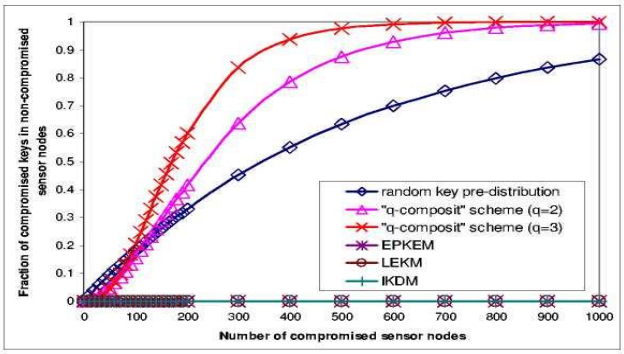

Figure 2: Fraction of compromised keys in non-captured sensor nodes vs. number of compromised sensor nodes

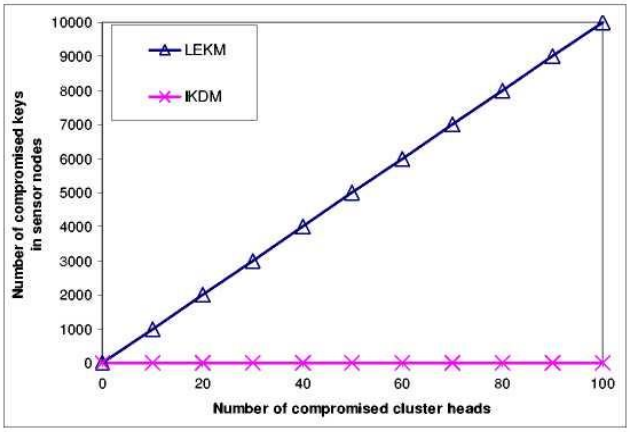

Figure 3: Number of compromised sensor keys vs. number of the compromised cluster heads in the network initialization phase

Figure 3 illustrates resilience against CH node capture attack in network initialization. In LEKM, each CH stores 100 SNs' secret keys, which can be compromised by each CH's capture. However, in IKDM scheme, only two 128-degree bivariate polynomial shares are stored in each CH, preventing CHs from knowing about SNs' secret keys. Even all 100 CHs are compromised, ensuring no pre-loaded SNs' keys are compromised.

In LEKM, group keys secure inter-cluster communication among CHs, but a single-point failure attack in a WSN environment can occur if a CH is compromised, allowing adversaries to crack communications

DOI: https://doi.org/10.54216/IJWAC.090105
Received: October 22, 2024 Revised: December 24, 2024 Accepted: January 21, 2025

between non-compromised CHs, potentially breaking the entire network's security. In IKDM, only polynomial shares are pre-loaded in CHs.

IKDM involves two CHs establishing a unique pairwise key before exchanging sensitive information. It prevents single-point failure attacks and ensures network security when no more than t CHs are compromised. The t-degree bivariate polynomial security property ensures network security when no more than t CHs are compromised. CHs have high battery power and large memory storage.

5. Conclusion

This dissertation addresses security issues in MANETs and WSNs, focusing on network security requirements, strategies, and cryptography mechanisms. It investigates mobile sink networks and wireless sensor networks, proposing a distributed anonymous secure routing protocol for routing security in MANETs. Two pairwise key establishment mechanisms are proposed for large-scale WSNs, and a realistic random key pre-distribution mechanism is investigated using random graph theory for robust sensing coverage and secure network connectivity.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Mousami Vanjale, Chitode, J. S. & Shilpa Gaikwad, 'Residual Battery Capacity Based Routing Protocol for Extending Lifetime of Mobile Ad Hoc Network', 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), pp.445-450.

[2] Muhammad Khalid Riaz, Fan Yangy and Imran Akhtar 2019, 'Energy Aware Path Selection based Efficient AODV for MANETs', Proceedings of 2019 16th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, pp.1040-1045.

[3] Nan Kang, Elhadi M. Shakshuki & Tarek R. Sheltami 2011, 'Detecting Forged Acknowledgements in MANETs', IEEE International Conference on Advanced Information Networking and Applications, pp. 488 – 494.

[4] Nidal Nasser & Yunfeng Chen 2007, 'Enhanced Intrusion Detection Systems For Discovering Malicious Nodes in Mobile Ad Hoc Network', In Proceedings of IEEE International Conference On Communication, Glasgow, Scotland, pp1155-1159.

[5] Onashoga, SA, Akinde, AD & Sodiya, AS 2006, 'A strategic review of existing mobile agent-based intrusion detection systems', Issues in Informing Science & Information Technology, vol.6, pp.669–682.

[6] Parth Patel, Rajesh Bansode & Bhushan Nemade 2016, 'Performance Evaluation of MANET Network Parameters Using AODV Protocol for HEAACK Enhancement', Elsevier Journals- Procedia Computer Science, vol.79, pp. 932-939.

[7] N. Sugirtham, R. Sherine Jenny, B. Thiyaneswaran, et al., (2024), "Modified Playfair for Text File Encryption and Meticulous Decryption with Arbitrary Fillers by Septenary Quadrate Pattern" International Journal of Networked and Distributed Computing, pp. 1-11, https://doi.org/10.1007/s44227-023-00019-4.

[8] K. Saravanan, S. Anthoniraj, S. Kumarganesh, T. Senthil Kumar, Martin Sagayam. K "Power Adjustment Algorithm for Higher Throughput in Mobile Ad hoc Networks" International Conference of Computer Sciences and Renewable Energies 2021 (ICCSRE 2021), July 23-24, at Agadir, Morocco. https://doi.org/10.1051/e3sconf/202129701064

[9] K. Saravanan, S. Anthoniraj, S. Kumarganesh, T.Senthil Kumar, Martin Sagayam. K "WMLP: Web-based Multi-Layer protocols for Emergency Data Transmission in Mobile Ad Hoc Network" International Conference of Computer Sciences and Renewable Energies 2021 (ICCSRE2021),July 23-24, at Agadir, Morocco. https://doi.org/10.1051/e3sconf/202129701065.

[10] Lalitha, S.P, Murugan, A. "Workflow scheduling and optimization using evaluationary method and deep learning algorithm in cloud" Multimedia Tools and Applications, 2024; Vol.83, pp. 78879–78896. https://doi.org/10.1007/s11042-024-18556-7

DOI: https://doi.org/10.54216/IJWAC.090105
Received: October 22, 2024 Revised: December 24, 2024 Accepted: January 21, 2025

[11] Lalitha, S.P, Murugan, A. "Performance Analysis of Priority Generation System for Multimedia Video using ANFIS Classifier" International Journal of Computational and Experimental Science and Engineering, 2024; Vol.10(4), pp. 1320-1328. https://doi.org/10.22399/ijcesen.707.

[12] S. Kumarganesh, S. Anthoniraj, T.Senthil Kumar, P.Elayaraja, et al. (2022), "A Novel Analytical Framework is Developed for Wireless Heterogeneous Networks for Video Streaming Applications" Journal of Mathematics, 2022(1) pp.1-7 doi:https://doi.org/10.1155/2022/2100883.

[13] K. Baskar, K. Muthumanickam, P. Vijayalakshmi & S. Kumarganesh, (2024), "A Strong Password Manager Using Multiple Encryption Techniques". Journal of The Institution of Engineers (India): Series B, pp. 1-8, DOI: https://doi.org/10.1007/s40031-024-01144-6.

DOI: https://doi.org/10.54216/IJWAC.090105
Received: October 22, 2024 Revised: December 24, 2024 Accepted: January 21, 2025