International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4048 Vol: 09, No. 01, 2025 ♦ PP. 31–33

Article DOI: https://doi.org/10.54216/IJWAC.090105

FULL LENGTH ARTICLE

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

Received: October 22, 2024 Revised: December 24, 2024 Accepted: January 21, 2025 ⋆ Corresponding author

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 weightage studies to continuously weigh the detection process. The performance of the suggested model is examined with regard to packet arrival ratio, throughput, end-to-end delay, communication overhead, and energy consumption. The framework aims to detect link flooding attacks in mobile ad hoc networks by strengthening intrusion monitoring and traceback capabilities.

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 out-of-range communication without fixed backbone infrastructure support [1]. This allows a network to be formed quickly by mobile devices that communicate through wireless links.

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 and suitable for applications where pre-existing infrastructure is unavailable or impractical.

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 centralized monitoring and stable infrastructure, malicious activity can spread quickly and affect routing reliability.

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 provide incorrect update information, leading to denial-of-service behaviour, route disruption, and link flooding.

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 approaches are therefore insufficient when nodes are mobile, resource-constrained, and exposed to adversarial behaviour.

© 2025 The Author(s). Published by ASPG. This article is licensed under CC BY 4.0.

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, including cryptographic protection, authentication, intrusion detection, and secure routing.

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 communicating parties.

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 [9].

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 [10]. Hashing functions can be keyed or non-keyed, compressing messages into message integrity codes without using keys or combining a message with a key to provide authentication. These cryptographic mechanisms provide a foundation for secure communication, but MANETs require additional mechanisms that can detect and respond to attacks arising from mobility and dynamic routing.

3. PROPOSED METHODOLOGY

The layer of mobile sinks, such as personal digital assistants (PDAs), self-organizes to form a mobile ad hoc network 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 of 5–20 metres. The proposed framework considers the interaction between mobile sinks, sensor nodes, and cluster heads in order to improve security and resilience against link flooding behaviour.

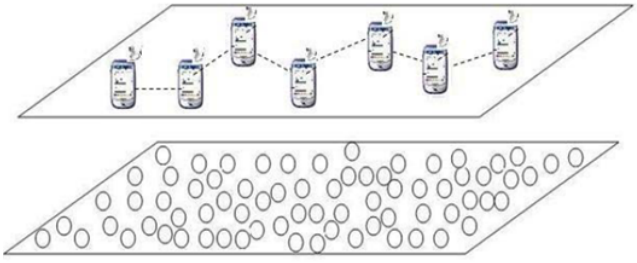

Figure 1. MSSSN architecture.

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 movement. This mobility improves data collection and reduces the distance over which constrained sensor nodes must communicate.

A user sends a query to a mobile sink, which checks whether 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 discovery in MANETs. The appropriate node collects data from its assigned region and communicates the response to the requesting user. This process supports distributed data access while limiting unnecessary energy consumption.

4. RESULTS AND DISCUSSION

Node capture attack poses a significant threat in wireless sensor networks because adversaries can physically capture sensor nodes to compromise stored secret information. Random key pre-distribution schemes may compromise communication between non-captured nodes. In LEKM and IKDM, no communication between non-captured nodes should be compromised when the adversary captures ordinary sensor nodes.

LEKM pre-loads secret keys in cluster heads during network initialization, allowing adversaries to compromise stored keys once a cluster head is captured. Figure 2 compares the fraction of compromised keys in non-captured sensor nodes against the number of compromised sensor nodes.

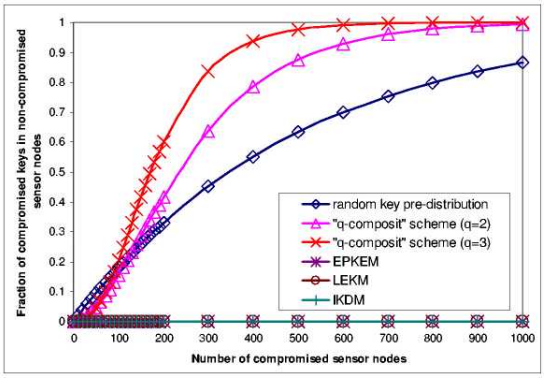

Figure 2. Fraction of compromised keys in non-captured sensor nodes versus number of compromised sensor nodes.

Figure 3 illustrates resilience against cluster-head node capture attacks in the network initialization phase. In LEKM, each cluster head stores 100 sensor nodes' secret keys, which can be compromised by the capture of each cluster head. However, in the IKDM scheme, only two 128-degree bivariate polynomial shares are stored in each cluster head, preventing cluster heads from knowing all sensor-node keys.

In LEKM, group keys secure inter-cluster communication among cluster heads, but a single-point failure attack in a wireless sensor network environment can occur if a cluster head is compromised. In such a case, adversaries can crack communications between non-compromised cluster heads, potentially breaking the entire network's security. In IKDM, only polynomial shares are stored, thereby reducing the effect of compromise.

IKDM involves two cluster heads establishing a unique pairwise key before exchanging sensitive information. It prevents single-point failure attacks and ensures network security when no more than t cluster heads are compromised. The t-degree bivariate polynomial security property ensures that the network remains secure when the number of compromised

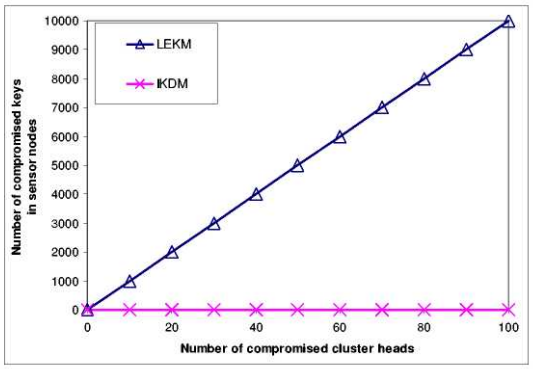

Figure 3. Number of compromised sensor keys versus number of compromised cluster heads in the network initialization phase.

cluster heads does not exceed the threshold t.

5. CONCLUSION

This dissertation addresses security issues in MANETs and wireless sensor networks, 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 MANET environments.

The proposed framework supports detection and mitigation of link flooding attacks by combining intrusion monitoring, honey-pot-based deception, and secure communication assumptions. The results highlight the importance of resilient key management and distributed detection in environments where nodes are mobile, resource-constrained, and vulnerable to capture attacks.

REFERENCES

[1] M. Vanjale, J. S. Chitode, and S. Gaikwad, "Residual battery capacity based routing protocol for extending lifetime of mobile ad hoc network," in *2018 International Conference on Advances in Communication and Computing Technology (ICACCT)*, 2018, pp. 445–450.

[2] M. K. Riaz, F. Yangy, and I. Akhtar, "Energy aware path selection based efficient aodv for manets," in *Proceedings of 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Islamabad, 2019, pp. 1040–1045.

[3] N. Kang, E. M. Shakshuki, and T. R. Sheltami, "Detecting forged acknowledgements in manets," in *IEEE International Conference on Advanced Information Networking and Applications*, 2011, pp. 488–494.

[4] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in *Proceedings of IEEE International Conference on Communication*, Glasgow, Scotland, 2007, pp. 1155–1159.

[5] S. A. Onashoga, A. D. Akinde, and A. S. Sodiya, "A strategic review of existing mobile agent-based intrusion detection systems," *Issues in Informing Science and Information Technology*, vol. 6, pp. 669–682, 2006.

[6] P. Patel, R. Bansode, and B. Nemade, "Performance evaluation of manet network parameters using aodv protocol for heaack enhancement," *Procedia Computer Science*, vol. 79, pp. 932–939, 2016.

[7] N. Sugirtham, R. S. Jenny, B. Thiyaneswaran *et al.*, "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, 2024.

[8] K. Baskar, K. Muthumanickam, P. Vijayalakshmi, and S. Kumarganesh, "A strong password manager using multiple encryption techniques," *Journal of The Institution of Engineers (India): Series B*, pp. 1–8, 2024.

[9] K. Saravanan, S. Anthoniraj, S. Kumarganesh, T. S. Kumar, and M. S. K., "Power adjustment algorithm for higher throughput in mobile ad hoc networks," in *International Conference of Computer Sciences and Renewable Energies*, Agadir, Morocco, 2021.

[10] K. Saravanan, S. Anthoniraj, S. Kumarganesh, T. S. Kumar, and M. S. K., "WMLP: Web-based multi-layer protocols for emergency data transmission in mobile ad hoc network," in *International Conference of Computer Sciences and Renewable Energies*, Agadir, Morocco, 2021.