e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 8, August 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI: 10.15680/IJMRSET.2024.0708021

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Novel and Hybrid Frameworks for Attack Detection and Secure Transmission in MANET

Bernisha, Dr.Jackson Daniel

UG Student, Department of ECE, Rohini College of Engineering, Palkumalm, Kanyakumari, Tamil Nadu, India

Professor, Department of ECE, Rohini College of Engineering, Palkumalm, Kanyakumari, Tamil Nadu, India

ABSTRACT: The nodes in MANET are constrained with limited power for their vital operations since the connectivity of the network will go down as soon as node energy gets exhausted. The proposed work focuses on trust based detect and computing to mitigate the effects of Black hole, and Wormhole attack. And used Optimized-AODV protocol, incorporates path accumulation during the route discovery process in AODV to attain extra routing information. In this proposed work, we apply a numerous techniques for secure and multipath data transmission. The techniques named as Hybrid Frameworks, such as Dynamic Route Selection, Mobile Agent Based Key Distribution (MAKD), and Packet Drop due to Attacker or Congestion (PDAC).

KEYWORDS: Mobile ad hoc networks, Dynamic Route Selection, Mobile Agent Based Key Distribution (MAKD), and Packet Drop due to Attacker or Congestion

I. INDRODUCTION

1.1 Mobile Ad hoc Network (MANET)

Mobile ad hoc networks, or MANETs for short, are also known as wireless adhoc networks or ad hoc wireless networks. They are often built on top of Link Layer ad hoc networks and provide a routable networking environment. Without a fixed infrastructure, they are made up of a collection of mobile nodes connected wirelessly to form a self-configured, self-healing network. Since the topology of the network is always changing, MANET nodes are free to relocate at will. Every node in the network acts as a router, forwarding traffic to other nodes that are specified. MANETs can function alone or as a component of a wider internet network. They create an extremely dynamic autonomous topology connecting nodes using one or more distinct transceivers.

II. RELATED WORKS

In a study by Wang et al. (2020), the researchers developed a deep learning model using Convolutional Neural Networks (CNNs) for fault detection in power systems. The model was trained on large datasets of voltage and current waveforms to identify and classify various types of faults, such as short circuits and grounding faults. The CNN's ability to automatically extract features from raw waveform data allowed for accurate and efficient fault detection. This work highlights the potential of deep learning in automating fault analysis, improving detection speed, and enhancing the reliability of power systems.

Zhang et al. (2021) proposed a fault diagnosis method for electrical grids using Gated Recurrent Units (GRUs). Their approach focused on analyzing time-series data from power grids, enabling the model to capture temporal dependencies in fault progression. The GRU model was particularly effective in predicting the evolution of faults over time, allowing for early detection and mitigation. The study demonstrated that GRUs could be applied to real-time fault monitoring, offering a significant improvement over traditional methods in terms of accuracy and response time, thus enhancing grid stability and resilience.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. RESEARCH METHODOLOGIES

The proposed work focuses on trust based detect and computing to mitigate the effects of Black hole, and Wormhole attack. And used Optimized-AODV protocol, incorporates path accumulation during the route discovery process in AODV to attain extra routing information. The systems labelled as Hybrid Frameworks, such as Dynamic Route Assortment, Mobile Agent Based Key Dissemination (MAKD), and Packet drop due to Assailant or Crowding (PDAC). A mechanism is established that produce randomized manifold routes. Below these policies, the pathways occupied through the bonds of dissimilar packages transformation over time.

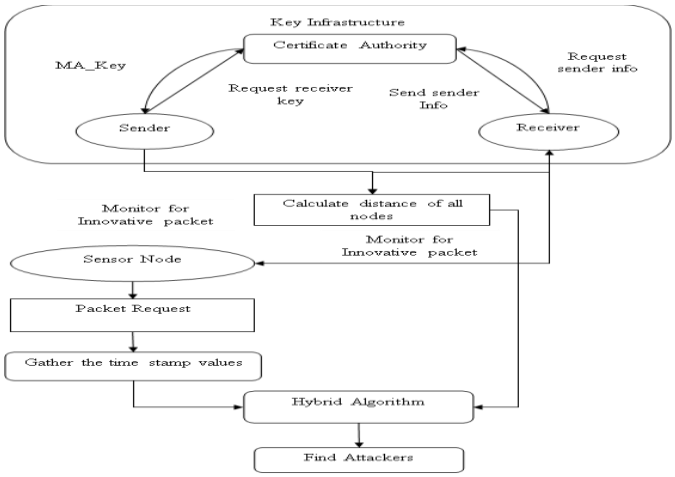
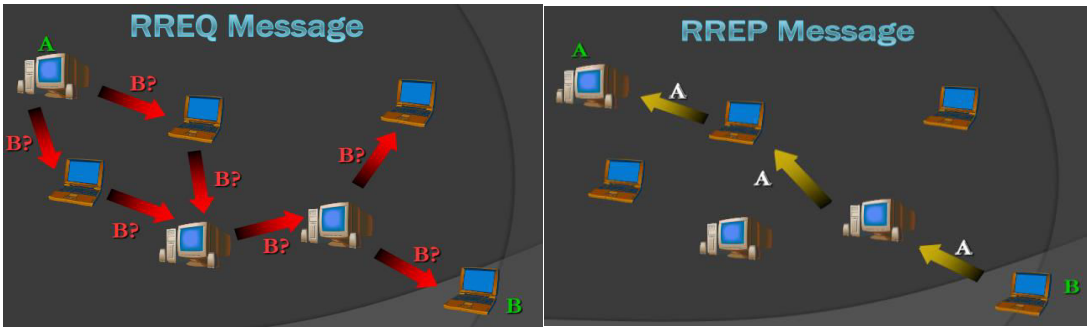


Fig 3.1 Proposed System Design



Dynamic Route Selection

In Dynamic Routing, Routing Protocols running in Routers continuously exchange network status updates between each other as broadcast or multicast. With the help of routing updates messages sent by the Routing Protocols, routers can continuously update the routing table when ever a network topolgy change happens.

Distance-vector Routing Protocols: Distance-vector Routing Protocols use simple algorithms that calculate a cumulative distance value between routers based on hop count.
Example: Routing Information Protocol Version 1 (RIPv1) and Interior Gateway Routing Protocol (IGRP)

Link-state Routing Protocols: Link-state Routing Protocols use sophisticated algorithms that maintain a complex database of internetwork topology.

© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI: 10.15680/IJMRSET.2024.0708021

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

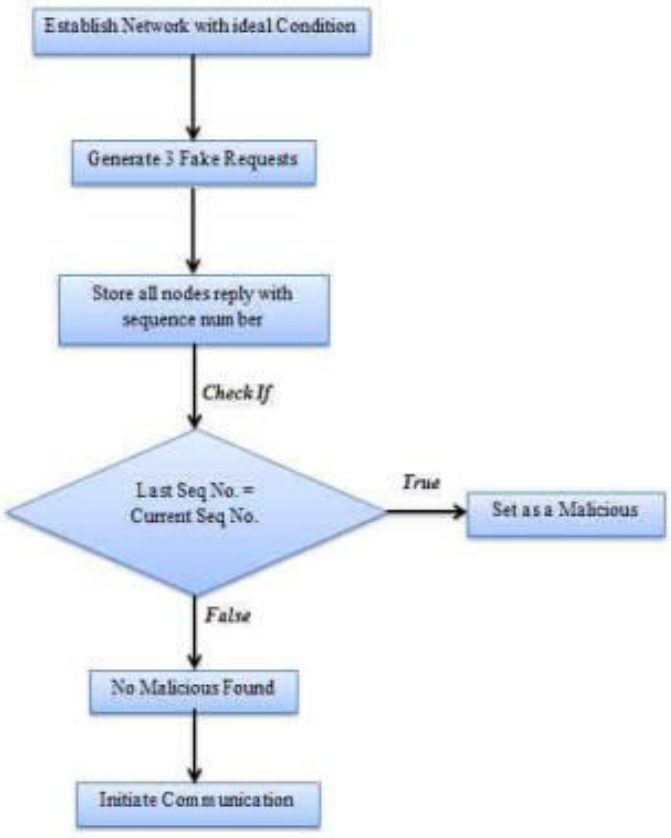
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Monitoring Agent Technique

The proposed the monitoring agent technique. The technique is based on capturing packets sent by neighboring nodes within a transmission range. All the nodes in a network collect information about their one hop neighbors within a certain period of time. The collected information include; the total number of packets transmitted from a particular node (WLi), the average number of transmitted packets from all its one hop neighbors (AWL), the packet drop rate of a particular one hop neighbor (DRi), and the average packet dropping rate by all its one hop neighbors (ADR) which are used for identifying a malicious node. The concept and S is the monitoring agent. S uses information collected from its neighbors to determine whether there are legitimate or malicious nodes.

To reduce false negatives (whether a node dropped packets maliciously or due to traffic problem), AWL (average of packet transmission by neighboring nodes) is calculated. In table 1, the AWL during a certain period of time is 224. The total number of packets broadcasted by a malicious node A during that period was 100 and this was lower than the average number of packets, so it had a high packet drop rate. Thus, monitoring node S determined that node A was maliciously dropping packets and an alarm message was sent to the entire network so as to inform the source.



IV. EXPERIMENTAL RESULT AND DISCUSSION

This study used ns-2 as the network simulator and conducted numerous simulations to evaluate the proposed performance. All sensor nodes are randomly scattered with a uniform distribution. The location of the sink is randomly determined. This study evaluates the routing performance under scenarios with different numbers of nodes.

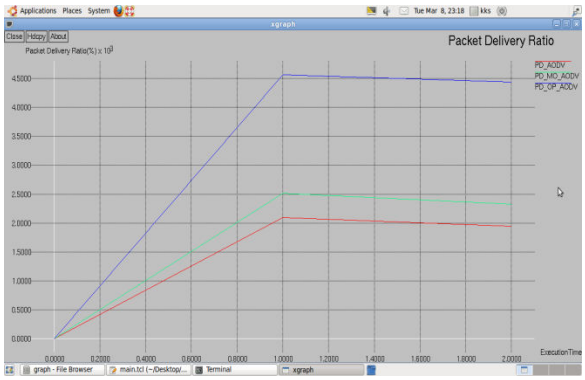
© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI: 10.15680/IJMRSET.2024.0708021

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

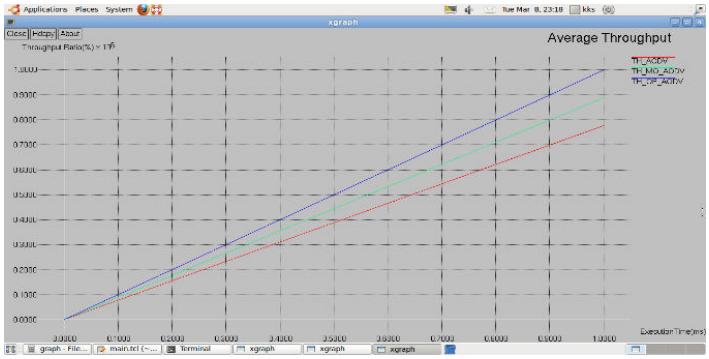
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. Packet Delivery Ratio:



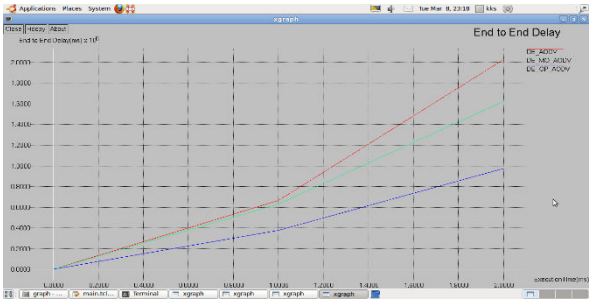
Here we comparing packet delivery ratio for Existing, proposed and Modification. In our modification life time ratio increased comparing to existing and proposed methods.

2. Throughput Ratio:



Here we comparing Throughput ratio, it's about successive rate of our modification (high energy efficient, reduce energy consumption and Delay).Our modification having high throughput ratio comparing to existing and proposed frameworks.

3. End-to-End Delay:



Here we comparing Delay ratio, it's about time delay and communication (high energy efficient, reduce energy consumption).Our modification low delay ratio comparing to existing frameworks.

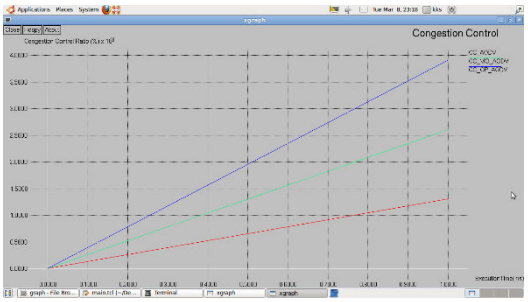
© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI: 10.15680/IJMRSET.2024.0708021

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

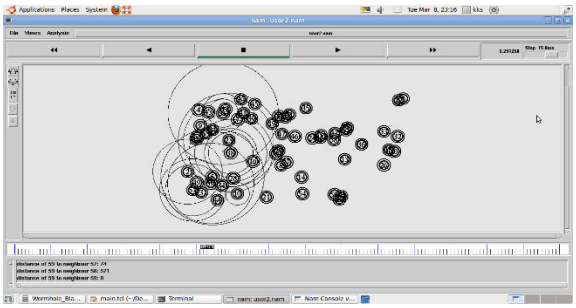
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

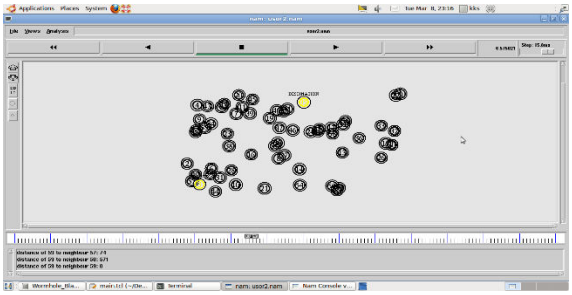
4. Congestion control:



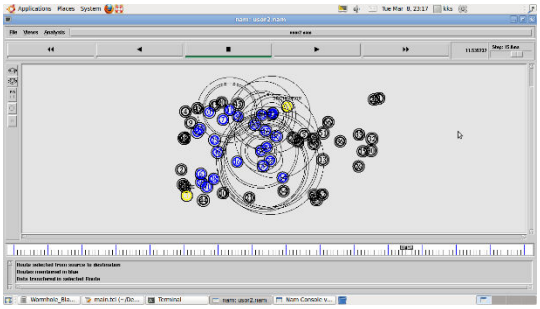
Here we comparing Congestion control, it's about Congestion control and communication (high energy efficient, reduce energy consumption).Our modification low Congestion control ratio comparing to existing frameworks.



Initial node construction & sending hello packets for getting neighbor location



Give source and destination and transmission using sensor nodes

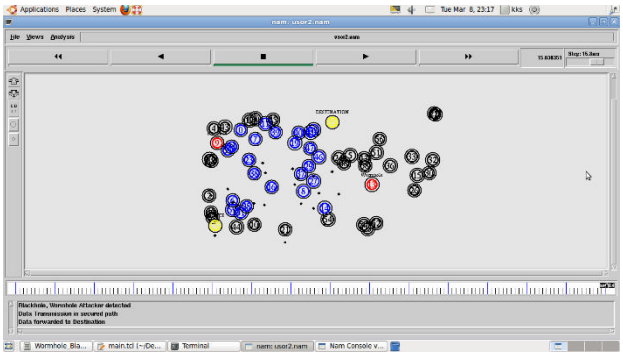


Path selection between source and destination

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Data transmission using secure path.

The proposed system addresses these gaps by enhancing both energy efficiency and security. It employs advanced protocols to ensure energy is transferred efficiently between nodes, extending their operational lifespan and reducing the need for frequent recharging. This is especially advantageous for remote or hard-to-access locations.

In terms of security, the proposed system integrates sophisticated malware detection algorithms. These algorithms scan for and identify malware within the network, isolating and ignoring infected nodes or data packets. This proactive approach ensures that only secure, clean data is transmitted, significantly boosting the network's overall security and reliability.

In essence, while the current system is effective in data transmission, the proposed system improves upon it by ensuring efficient energy use and robust malware detection. This dual enhancement makes the proposed system a more sustainable and secure solution for modern network operations.

V. CONCLUSION AND FUTURE WORK

In this work, we used a numerous technique for secure and multipath data transmission in WMSN. The techniques named as Hybrid Frameworks, such as Dynamic Route Selection, Mobile Agent Based Key Distribution (MAKD), and Packet Drop due to Attacker or Congestion (PDAC). In this framework, we used OAODV Routing for Route Detection and Route Maintenance. Under the Anonymous Detection management, in this framework we used Mobile Agent Based Key Distribution a security key management for secure path selection criterion is designed to select the most reliable and shortest path in terms of Routing available resources. Simulation results show that the generated routes are also highly dispersive and energy efficient, then MAKD is scalable and with less memory overhead. And PDAC, the effectiveness of provenance is secured by avoiding packet drop attacks.

In future, improve this process security as digital signature security frame work and our proposed security scheme for centralized topology networks, so in future we improve this security using digital signature security technique for decentralized large level networks topologies.

REFERENCES

[1] P. Kumar, S. Lee, and H. Lee, "E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," Sensors-Basel, vol. 12, pp. 1625–1647, Feb. 2012.
[2] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks,"IEEE J. Biomed. Health Informat., vol. 18, no. 1, pp. 316–326, Jan. 2014.
[3] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," IEEE Sensors J., vol. 16, no. 5, pp. 1368–1376, Mar. 2016.
[4] T. H. Chen and W. K Shih, "A robust mutual authentication protocol for wireless sensor networks,"ETRI J., vol. 32, no. 5, pp. 704–712, 2010.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[5] X. H. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare,"J. Netw., vol. 6, no. 3, pp. 355–364, 2011.
[6] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity,"Security Commun. Netw.,vol.9, pp. 2643–2655, 2015.
[7] F. Wu and L. Xu, "Security analysis and improvement of a privacy authentication scheme for telecare medical information systems,"J. Med. Syst., vol. 37, no. 4, pp. 1–9, 2013.
[8] L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," J. Med. Syst., vol. 39, no. 2, pp. 1–9, 2015.
[9] Information technology—Smart transducer interface for sensors and actuators — Part 7: Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) formats, ISO/IEC/IEEE Std 21451-7, pp. 1–82, 2011.
[10] A. K. Das and B. Bruhadeshwar, "An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system,"J. Med. Syst., vol. 37, no. 5, pp. 1–17, 2013.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com