International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I7P239

Volume 70 Issue 7, 377-387, July 2022

Original Article

An Application Data Privacy Preservation Strategy for MANET 2ACK to Identify and Mitigate the Effect of Routing Issue

D. Naga Tej[1], K V Ramana[2]

[1]*JNTUK, Kakinada & Gayatri Vidya Parishad College of Engineering, Madhurawada, Visakhapatnam, Andhra Pradesh, India.*
[2]*JNTUK Kakinada, Kakinada, Andhra Pradesh, India.*

[1]nagatej09@gmail.com

Received: 06 May 2022 Revised: 07 July 2022 Accepted: 18 July 2022 Published: 27 July 2022

Abstract *- Data privacy is concerned when transferring sensitive data over a multi-hop channel in Mobile Adhoc Networks (MANET). It is likely that undesirable data exposure could result in privacy violations and that this information will be used to launch various attacks against diverse targets. There are various ways for the confidentiality of Adhoc Nodes information may be protected, each of which is addressed in further detail below. However, the drawback of using these solutions in a MANET is that it requires high computational costs and significant time delays. A computational intelligence-based data privacy solution has been provided to keep the processing power to an absolute minimum. When defining the data characteristics that should be kept secret, it uses a data anonymization technique based on rough set theory to determine such characteristics. A diverse collection of trustworthy and neighbor nodes is selected during each routing phase, with the number of routes available changing dynamically. Data is delivered and received as a result of this selection. It is also stated that the identity of the recipient will remain anonymous. Various routing with network sizes was used to accomplish the work, which was completed by simulating it in various network sizes. The outcome of this study is quite beneficial in most circumstances for the Application of Data Privacy Preservation Strategy, which was the subject of this study.*

Keywords *- 2ACK, MANETs, Routing fault, Selfish node.*

1. Introduction

Some computers in a network may want to calculate a function using their private inputs. However, MANET 2ACK may not use these inputs to be visible to other computers in the network under certain situations. Secure Multiparty Computing (also known as SMC for short) describes this kind of computation (SMC). Changing the data inputs or using anonymization techniques in mobile ad hoc networks may help to alleviate SMC-related problems in mobile ad hoc networks (MANET). Permanent infrastructure for MANETs, wireless networks of mobile computers, is not necessary to function well. Bluetooth, IEEE 802.11, or Hiperlan are all options if the mobile nodes want to connect. These components may be of use to both hosts and routers. Security difficulties arise due to the changeable topology of the MANET, the lack of dependable wireless connection, and the dynamic nature of the environment. Identifying the nodes that use identification and producing practical credentials are two tasks that must be completed. Aside from that, there are concerns about the architecture's security and privacy protections. Therefore, it is necessary to provide a method that prohibits nodes from knowing the identities and credentials of their peers. Preserving people's privacy in a MANET is not straightforward and requires careful planning and implementation. There is currently minimal thought paid to security and privacy considerations regarding routing protocols. To prevent unwanted access in different encryption systems, it is sometimes necessary to use an authentication mechanism between nodes to avoid data theft. It is essential for maintaining service availability and operation in service-oriented MANETs. Because the applications used to create and use an ad hoc network are so diverse, the security needs for each differ from one another. The rules of engagement in mobilized combat are distinct from those that govern a conventional business meeting. Consequently, a complete security strategy for MANET cannot be implemented in its current form. Each application must have its security architecture, separate from the others. Although the security community still has much work to do, this work will be incorporated into current standards as MANET becomes more extensively utilized in the real

world. This presentation will demonstrate how to use SMC techniques to keep computations confidential. [1].

The security of suspicious MANETs, a subset of MANETs in which the nodes do not trust one another, is a crucial source of worry for researchers. MANET 2ACK may use privacy protection in suspected MANETs to launch attacks without actual attackers' detection. As stated in further depth below, this study suggests a strategy for protecting privacy when using position-based routing for questionable MANETs discussed in greater detail below. Because PPP and MNR methods are included in standard position-based routing protocols, nodes may have customizable privacy protection, and networks may have adjustable security. Aside from that, node control location privacy is possible using the proposed method. [2] This technique may defend nodes against hostile insiders and spoofing assaults if a suspect MANET is used. It has the additional benefit of shielding the Data Privacy Preservation Strategy from outsiders who want to damage MANETs.

It is impossible to maintain track of where people are at any one moment in CR-MANETs since there is no trusted central authority imposing privacy-preserving procedures. It results in decreased privacy for the devices connected to the network due to each device giving more information to the network due to the use of CR-MANETs with more than one channel [3].

2. Literature Review

Wireless networks are sometimes called "distributed networks," making it impossible to pinpoint where each node or participant is physically situated. MANETs result from their lack of infrastructure and resources. MANET 2ACK utilize mobile devices to access a wide range of services and information in several contexts. Personnel from several mobile networks who want to interact must first create mutual trust before MANET 2ACK may communicate with one another. There are several examples of how to set up trust overlays in MANETs, keep the Data Privacy Preservation Strategy up to date, and advise on safeguarding one's data. To work effectively, computer hardware reliability is becoming more critical for open systems, such as laptops and smartphones. It is feasible to use any mobile device to execute the necessary access control, which is a critical component of the solution plan. The MANET still has several significant challenges to overcome, such as developing security rules that work across several administrative domains and how to instill faith in the MANET. These are only a few examples.

The computers in a network may want to calculate a function using their private inputs, but MANET 2ACK will not want to share these Adhoc Nodes inputs simultaneously. Secure Multiparty Computing (also known as SMC for short) describes this kind of computing (SMC). It is feasible to adjust the data inputs or utilize anonymization techniques in Mobile Ad hoc Networks to alleviate SMC issues in these networks (MANET). As far as functionality is concerned, MANETs, which are wireless networks of mobile computers, do not necessitate using any fixed infrastructure. Mobile nodes can connect via various protocols such as Bluetooth, and IEEE 802.11 versions, which may benefit hosts and routers in certain circumstances. Security difficulties arise due to the changeable topology of the MANET, the absence of consistent wireless connection, and the dynamic nature of the surrounding environment, among other factors.

Identifying the nodes that use identification and developing a mechanism for generating viable credentials must be devised and tested. Aside from that, there are concerns about the security and privacy of this architecture. Therefore, it is necessary to provide a method that prevents nodes from finding the identities and credentials of other nodes. Preserving people's privacy in a MANET is not straightforward and requires careful planning and execution. Security and privacy considerations are given little attention regarding routing protocols. To prevent unwanted access in different encryption systems, it is sometimes necessary to use an authentication mechanism between nodes to avoid data theft. It must be considered to maintain service availability and operation in service-oriented MANETs. The security requirements of an Adhoc network differ on the application for which it is being utilized.

In contrast to a conventional business meeting, military battles are controlled by a particular set of rules and laws. As a result, there is currently no way to develop a comprehensive security plan for MANET. Each application must have its security architecture, separate from the others. There is still more work to be done by the security community, and when MANET becomes more extensively utilized in the real world, this work will be included in the current standards. In this study, as seen in figure 5, these methods may be used to keep private information safe while computation is conducted.

Substantial work has been done on MANETs, and this effort has continued to this day. The autos connect forms an Adhoc communication network called VANET (Vehicle Ad Hoc Network). While improving the navigation system's intelligence, the system's security must not be threatened. According to a comprehensive analysis of the literature, the work necessitates using a navigation system that is both clever and safe in its operation. This study covers the development of a navigation system that is effective in real-world situations. This approach addresses a variety of difficulties, including authentication, secrecy, and privacy of the car and its driver, among others. The suggested system's performance is assessed in terms of Quality of Service (QoS) (Quality of Service). While drivers use this system,

MANET 2ACK may be confident that it will be given an accident-free route since it considers real-world road conditions when looking for the shortest route to their destination. Another benefit is that broadcast messages are given more weight than other communications.

This technology is becoming more critical because of its capacity to transport data networks from one vehicle to another in circumstances where wired solutions are challenging to establish. Adhoc networks are set up in circumstances when it is not feasible to install the required sorts of hardware and network equipment regularly. Every member of a Vehicular Ad hoc Network (VANET) collaborates as data terminals and network routers without a centralized point of control, therefore eliminating the need for a centralized point of control in the first place. VANETs are a kind of wireless ad hoc network that is very mobile and has the potential to change its topology in a concise amount of time. VANETs are becoming more popular [4].

Consequently, MANET 2ACK may be used in various applications due to its versatility. It may be able to perform various tasks, including warning systems, enhanced navigation systems, entertainment, and information applications, to name a few, if MANET 2ACK has access to the necessary technology. A significant amount of time and effort is being expended to assist persons in better understanding the challenges of vehicular communication. The network's design, protocols for the physical and link layers, and routing algorithms are all topics that people are interested in these days. According to the DOT, the ability to communicate securely between vehicles and between vehicles and infrastructure is essential for vehicular communication systems' effective and safe operation. Node communications may be kept private and protected from people who might be interested in reading Data Privacy Preservation Strategy. Cryptography is used to encrypt communications to only be read by those with access to a private or public key associated with the message. Communication between nodes in MTA is protected by private key encryption [5], implemented in a method (Multilingual Translation Algorithm) [6].

Sharing information requires the other person's trust, which can only be gained through time and effort. Using trust management to assist users in picking safe channels will help mobile ad hoc networks do better in their operations. Using trusted routes and building a trust management hierarchy is crucial for developing trust in a business environment. For people to have faith in communication networks supplied by all levels of government, MANET 2ACK must do so. When it comes to mobile ad hoc networks, managing trust is essential for success. The definition of trust in a dispersed network scenario may be achieved by mutual collaboration and overall reputation, a dependability index, a friendship mechanism, and other qualities that make it possible for all mobile nodes to have an overall trust coefficient. The efficiency of trust management systems varies greatly depending on how MANET is conceived and implemented. A detailed discussion of trust management and trust-building components has been conducted as part of this research study. In the future, it is feasible that the combination of MANET and secure multi-party computing will substantially impact trust results and how MANET is used. It is critical to consider protecting people's privacy while spreading trust in mobile networks. The SMC protocols learned a valuable lesson about this while developing because MANET had to deal with many diverse communication partners [7] during their development.

Wireless ad-hoc networks, under their open nature, frequently changing topology, and lack of a centralized infrastructure, offer a considerable security risk to the network's users. Consequently, MANET is more vulnerable to assaults than other types of networks are. It is possible to launch an attack quietly or forcefully. As a result of the fact that it is listening in on data packets, the passive attack in a network environment is difficult to detect. Due to this, a significant concern among the MANET community has been the privacy of data packet payloads. Military applications, privacy disputes, and other high-stakes events, to name a few examples, are all situations that may arise. Symmetric cryptography was used, and five proposed modifications to the AES algorithm were made in key generation. Based on a multi-chaotic system, a new sub byte, new shift rows [8], add two XOR [9], add-Shift cyclic [10], and a new sub byte [11]. Symmetric cryptography was also used in this research.

A decentralized network, such as peer-to-peer networks, physical ad-hoc networks, or other decentralized networks, cannot be entirely controlled by a single person. Attacks against these networks, especially those targeted at gaining Adhoc Nodes information from individuals who use Data Privacy Preservation Strategy, are particularly vulnerable to success. The privacy of its customers is used to protect the work, using two principles. To begin, build groups of individuals who can put trust and who will support. Methods like anonymization are also used to secure users' identities while simultaneously ensuring that their trust in the organizations to which MANET belong does not get undermined. In this study, the communication model built as a consequence of the findings is referred to as "HypAnoCom." It is built on the hypergraph paradigm, which acts as the system's basis [12]. Conversations between participants from various cultural backgrounds are permitted without the participants' identities being revealed. The team created an algorithm that may be utilized to discover the shortest possible transversals. MANET is used to protect the privacy of people or businesses. Developing a routing system based on a selective hierarchy is underway to

guarantee that communication is maintained. The proposed technique, which protects identity, location, and safety, may help avoid potential problems. The proposed method's dispersed and dynamic nature may be helpful to people who, for example, use ad hoc networks and peer-to-peer networks to communicate. Using hyperedges at each hop in the proposed model allows us to deal with churn more effectively [13].

Specific large-scale MANET applications, such as those used by the military, focus significantly on privacy and anonymity to maintain their security and privacy. Because of these applications' administrative or routing needs, MANET is more likely to establish networks using various varied and hierarchical approaches. Flat anonymous routing systems become more time-consuming when the number of public-key activities on the network rises in proportion to the network size, which suggests that the amount of time it takes to use the Data Privacy Preservation Strategy grows faster. It has a detrimental influence on the performance of routing and data transmission systems. This research specifically illustrates how to set up a new hierarchical anonymous on-demand routing system to tackle this problem. The routing and data delivery security assurances include security guarantees for intra- and inter-group anonymity and security guarantees for data integrity, which are all included in the routing and data delivery security assurances. Due to the hierarchical network architecture, it is a great choice for large-scale MANET applications due to these characteristics [14].

Apps such as VANETs, which let autos speak with one another on the road, are being developed to increase road safety. In the recent past, wireless and mobile communication are becoming more interested in virtual private networks (VANETs). People using VANETs cannot keep their data private or safe because VANETs suffer from the same security concerns as other networks, making it difficult to preserve privacy and security. VANETs are also susceptible to data breaches. For various reasons, protecting the network in VANETs is very important. The segmentation of autos into separate groups makes it possible to communicate securely from beginning to end during the journey. Vehicles traveling together or in different groups that have permitted each other to transmit security and non-wellness data are safe and secure. This is the case for most group communications, and it is the case most of the time. To ensure communication security, the cluster head should be chosen from among the most trustworthy nodes. Each member of the group is given a "key" (KEK) as well as an "encryption key" to keep their conversations private and confidential (TEK). Many different ways have been devised to manage group keys to keep data safe in a group network environment. There are several benefits to VANET and its members from the work that has already been completed on this site. Several studies have been carried out in wireless networks to explore the aspects of selfish nodes from various angles, and the results have been published. The bulk of this study focuses on one of the three areas below: education, health, and environment [15]. Mechanisms of encouragement, detection techniques, and impact studies are covered in this book section. The sixth point is as follows: Researchers investigated the various strategies for identifying selfish nodes in MANETs developed over the years as part of one of their studies. The Pathrater and the Watchdog were two ways that MANET looked into further. [16] Vij and his associates. Using game theory, the Pathrater methodology may identify misbehaving nodes at the forwarding level, while the Watchdog method use game theory to detect selfish nodes at the forwarding level, as described below. MANET proposed a system that can monitor and detect selfish nodes while using the battery as a limited resource, according to Lupia proposed different research works. On the other hand, the energy consumption of the nodes is not taken into account by this approach [21]. According to another study, RoselinMary devised an algorithm that might reduce the energy consumption of the nodes while still enabling the Data Privacy Preservation Strategy to be identified. [17] RoselinMary and her associates. This group consists of a total of eleven individuals. Ad hoc networks' packet forwarding and other features are used to detect denial of service (DoS) attacks before MANET may take place. Singh algorithm, known as EAPDA, has been enhanced and modified throughout the years. It was first released a few years ago and has been refined even more [18].

Kim developed a system for identifying security risks in a multi-class environment using a support vector machine setting with many different types of assaults and classes of attacks. Additionally, Ilavendhan [19] investigated the many methods for detecting denial-of-service (DoS) attacks in virtualized networks that have been developed over the years. The study focuses on the detrimental repercussions of selfish nodes on the overall performance of a network. Collaboration between these nodes is essential for preventing Data Privacy Preservation Strategy from causing damage to the network. It is possible to utilize several incentive mechanisms to encourage the network to perform effectively. Here are some examples. Here are a few examples. The reputation-based reward mechanism is among several incentive mechanisms that encourage cooperative behavior.

To put it another way, this concept works by rewarding nodes with higher reputation ratings for cooperating more. Based on the work by Wu proposed [20], an incentive mechanism based on reputation has been devised that may be used in MANETs. According to another study, a system that combines pricing and resource systems to encourage network cooperation might be developed. In another study, Lai developed a secure reward system that might be used in

highway VANETs. The team also built a reputation system, which may be used to penalize both malicious and beneficial nodes equally depending on their behavior. The self-interested nodes may choose to share their resources with the rest of the network rather than being excluded from it. Because of the nature of reputation-based incentive schemes, MANET relies on past knowledge about the nodes' behavior to assess the success of the scheme in question [21]. An incentive system based on credits has been proposed by the authors of this study, which require nodes to transfer their packets to the network's security module in return for credits. MANET has developed an approach that may be used to detect self-serving nodes. Nodes that are not cooperative are penalized using the Tit-for-Tat system, which uses a barter-based exchange system. Depending on its preferences, a node may behave as either a cooperative or a selfish actor when using this strategy [22].

In some cases, such as when dealing with auctions, the concept of a barter-based approach may also be used as a tool in game theory. To implement this method, techniques from the fields of reinforcement learning and game theory may be used. Similarly, Wu combined a price-based system with a reputation system, and Li [23] [24] devised a technique for recognizing and deterring selfish nodes in MANETs, which was subsequently enhanced. We used both of these techniques. In the past, a technique for increasing network cooperation based on evolutionary game theory was proposed, but it has since been abandoned. MANET used Yang's [25] game-based optimal pricing technique to represent data offloading in VANETs for their investigation. This method was used to illustrate data offloading in VANETs. AI-Terri provided the suggestion below [26]: To effectively encourage collaboration at the MAC layer in VANETs and MANETs, two TFT-based strategies were devised and implemented. Both of these tactics were successful. The goal of using these strategies is to boost the detection of misbehavior inside the network by rewarding or discouraging nodes performing incorrectly, with the eventual goal of increasing the network's overall efficiency. Unfortunately, no study has been undertaken to determine whether or whether the performance of the network is impacted by nodes that just care about themselves. Even though several research has been conducted on the effects of node selfishness on the network, few studies have been conducted on the effects of node selfishness on network performance in mobile ad hoc networks. According to the results of Kyasanur researchers, unethical behaviour on the part of certain hosts may come from their failure to adhere to the network's regulations. It was reported earlier [27]. Lei [28] suggested various possible ways of dealing with the misbehaviour of the nodes depending on the data they collected. The MANET team tested their theories using two widely utilised routing technologies.

Next, the authors' Xu analysed two distinct types of nodes to see how the selfishness of individual nodes influenced the network. One of the Data Privacy Preservation Strategies has been assigned to the type-1 category, while the other has been assigned to the type-2 category. Selfish nodes, like type-1 nodes, do not send or receive packets, but selfish nodes, like type-2 nodes, do not perform routing operations [29]. After extensive research on this topic, the authors concluded that node selfishness is more detrimental to the performance of type-2 networks than type-1 networks [30]. As a direct result, MANET produced many types of selfish nodes to explore the consequences of these nodes on the rest of the system. This study revealed that selfish behaviour harms the quantity of energy utilised in opportunistic networks. This conclusion was reached as a result of the study. Researchers from various universities have shown that the overall amount of energy in a network may have a considerable influence on the willingness of its nodes to interact [31]. Despite their best efforts, the research authors could not analyse the effect of node selfishness on the network's total energy consumption using MANET. Unfortunately, this issue has not yet been resolved [32].

3. Proposed Method

It was determined which I-hop neighbor nodes were trusted based on their trust qualities by the researchers that carried out this research using rough set theory. The researchers also looked at the relationships between data characteristics (for anonymization). The following resources are available.

RsrAvl measures how many resources, such as bandwidth and battery power, are available at any time [33]. In addition to the Node Traversal Time (NNTT) and link stability between nodes, the dependability of a node's delivery rate and the number of route failures, which is referred to as Node Reliability, are influenced by the Node Traversal Time (NNTT) and link stability between nodes (NRel) When a node in a MANET transmits and receives packets, the history of that node is recorded. Node History (NHis) is based on the number of packets sent and received by the node in a MANET (due to malicious behavior). A record is an actual value that must be sent; a type is a form in which data is organized. Time is the amount at which the data was captured. The following definitions apply: Entity - an entity to which data pertains, such as a gadget or a person; and Effect demonstrates the impact that data has on someone or something. The proposed architecture is furnished as in figure1.

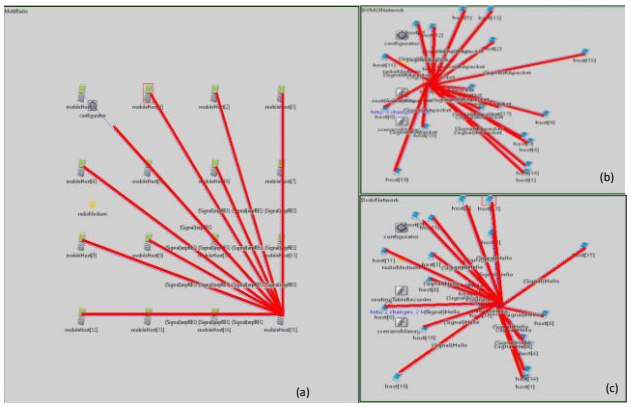

Fig. 1 Proposed Secure MANET Architectures using (a) MultiRadio, (b)DYMO Network, (c) DSDV

4. Data Privacy Preservation Strategy For MANET 2ACK

For example, 2ACK's pseudocode uses the triplet N1 N2 N3 throughout this article [34]. Assume that node N1 is the source, node N2 is the intermediate, and node N3 is the destination. It is important to remember that these codes are carried out on both the sender and the receiver of 2ACK packets [35, 36]. It is currently known as 2ACK. It is time to divide the start time by the time allotted for the acceptance acknowledgment [37]. Remove 48 bytes from the length of any communication packet that has a length that is more than 48 bytes [38]. Make use of the hash function to keep the message secure. Utilize Cpkts++ so the message and hash key may be sent [39].

Step - 1. Receive a packet with 2ACKs.
Step - 2. As long as (2ACK time) is more than WT, Cmiss++;
Step - 3. 48 bytes in length
- i. To protect the message, use the hash function. Cpkts++: Send a message and a hash key, then check the message.
- ii. Sender: I-Node got a 2ACK packet from the server.
- iii. If (2ACK time > WT), then Cmiss++; if not,
- iv. read the message from source N1 at node N2. If (Alter) is true, then do this (true).
- v. Insert fake character bytes.
- vi. Send it to N3 so MANET can look at it. N3 sends the 2ACK back to N1.
- vii. Don't change: if not
- viii. N3 should get it soon. Send 2ACK to N1 to get it from N3.
- ix. end

Step - 4. end
Step - 5. N2 sent a message to node N3. At the same time, node N3 read the message.
Step - 6. The destination name and hash code should be taken out of the list. People need to figure out how to read the message.
- i. Make sure that N2 gets a 2ACK packet.

Step - 7. end
Step - 8. Between N1 and N3, there are a lot of similarities between two.
- i. Even though it's true that it's true
- ii. If the hash code of the source message doesn't match the hash code of the destination message, then it won't be sent.
- iii. Link is being dishonest, and the secrecy has been broken;
- iv. end
- v. If ((Cpkts)d and (Hash code of source message)! = (Hash code of destination message), then this is a match. If only then (if only)
- vi. Confidentiality has been breached since the link has been running.
- vii. end
- viii. To say it another way: When the condition is met, the ratio of missed calls to missed calls is greater than the ratio of missed calls to missed calls.
- ix. Link is behaving weirdly.

Step - 9. end
- i. if the hash code of the source message and the hash code of the destination message match up
- ii. The link works as it should.
- iii. end

Step - 10. end

5. Experimental Analysis

The collected findings from the simulation on OMNET++ are explained in this section only via graphical representation [40,41]. Figure 2 depicts the relationship between the number of delivered packets and the total number of errors. The Pm has been updated from 0 to 0.4, indicating that all the nodes are acting as MANET are supposed to (40 percent of the nodes are misbehaving). When Pm is zero, many packets are delivered to their intended destinations. (There are no problematic nodes.) The number of packets transmitted decreases as the size of Pm increases. Even with Pm = 0.4, the 2ACK technique delivered more than 90 percent of the data packets. In this case, there were four different values for the R2ack acknowledgment ratio: 0, 0.2, 0.5, and 1. By contrast, R2ack does not affect 2ACK's PDR.

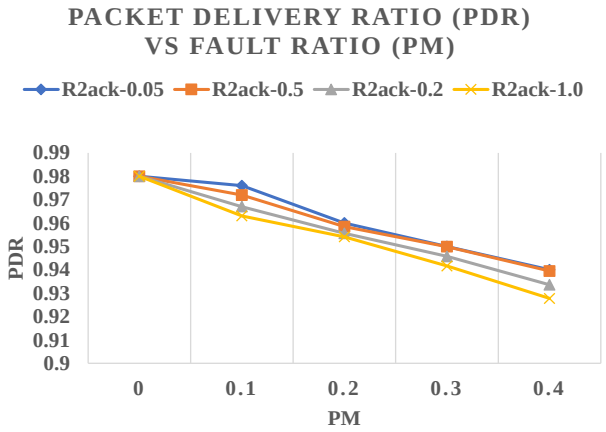

Fig. 2 Packet delivery ratio (PDR) versus fault ratio (Pm)

Depending on how high the acknowledgment ratio is, the routing overhead (RO) of the 2ACK method fluctuates. Figure 3 shows how this works. (R2ack). P-values might be between 0 (all nodes behaved) and 0.04 (some nodes did not act). (About 40% of the nodes are acting inappropriately.) Specifically, the methodology investigates how much time it takes to compare the 2ACK routing scheme's overhead with various R2ack values. As a result, when R2ack is 1, the 2ACK approach has the highest overhead. A large number of 2ACK packets are transmitted over the network, which causes this problem. When the value of R2ack decreases, the amount of routing overhead decreases. The R2ack module of the 2ACK system contains a "knob" that adjusts the amount of routing overhead used.

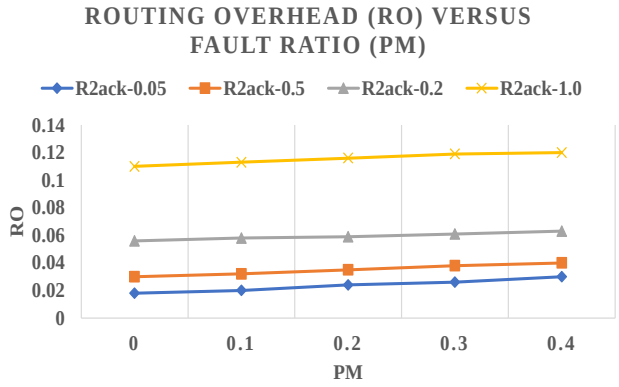

Fig. 3 Routing overhead (RO) versus fault ratio (Pm)

Figure 4 depicts the relative throughput of the 2ACK method at various acknowledgment ratios, or R2ack, for various acknowledgment ratios. P-values might be between 0 (all nodes behaved) and 0.04 (some nodes did not act). Almost 40% of the population is acting inappropriately.

Table 1. Routes, Times, and Packets that were sent

Route	Time Slot1	Time Slot 2	Time Slot 3	Total Number of Packets
Route Path-1 N0 → N5	T = 0.5000 Packets = 1	T = 2.9300 Packets = 2	T = 5.3000 Packets = 8	11 Packets
Route Path-2 N0 → N1 → N3 → N5	T = 0.5300 Packets = 49	Packets = 0	Packets = 0	49 Packets
Route Path-3 N0 → N1 → N5	T = 2.0000 Packets = 31	Packets = 0	Packets = 0	31 Packets
Route Path-4 N0 → N2 → N4 → N5	T = 2.9900 Packets = 84	Packets = 0	Packets = 0	84 Packets
Route Path-5 N0 → N1 → N5	T = 5.2700 Packets = 1	Packets = 0	Packets = 0	1 Packet
Sent All Packets				**173 Packets**

Table 2. 2ACK, E2ACK, and IA-ACK Comparison

Technique	2ACK	E2ACK	IA-ACK
False misbehavior	Not detected	Detected	Detected
Overhead	Has overhead	Reduces overhead	Reduces overhead
Collaborative Node	Not detected	Not detected	Detected

This is where the proposal examines how well the 2ACK method performs when various R2ack values and different failure rates are used in conjunction. Throughput will be high when there are no flaws in the product or process. MANETs may be utilised to identify issues with their routing systems. Reducing the number of nodes to two and utilizing R2ack costs 0.05 cents.

Table 3. Packet delivery ratio (PDR) versus fault ratio (Pm)

PM	R2ack-0.05	R2ack-0.5	R2ack-0.2	R2ack-1.0
0	0.98	0.98	0.98	0.98
0.1	0.976	0.972	0.967	0.963
0.2	0.96	0.9585	0.9556	0.9541
0.3	0.95	0.94984	0.94572	0.9416
0.4	0.94	0.93946	0.933596	0.927732

Table 4. Routing overhead (RO) versus fault ratio (Pm)

PM	R2ack-0.05	R2ack-0.5	R2ack-0.2	R2ack-1.0
0	0.018	0.03	0.056	0.11
0.1	0.02	0.032	0.058	0.113
0.2	0.024	0.035	0.059	0.116
0.3	0.026	0.038	0.061	0.119
0.4	0.03	0.04	0.063	0.12

Every 100 packets that are transmitted requires the transmission of a 5 2ACK. When Pm or R2ack are increased, the rate of change changes less dramatically. The Pm value is 0.40 in this case, and the R2ack value is 1. This signifies that the 2ACK system has a throughput that is 90 percent of the total throughput.

Table 5. Throughput versus fault ratio (Pm)

Throughput	R2ack-0.05	R2ack-0.5	R2ack-0.2	R2ack-1.0
0	0.99	0.98	0.97	0.96
0.1	0.978	0.97	0.95	0.94
0.2	0.96	0.95	0.94	0.93
0.3	0.945	0.938	0.922	0.91
0.4	0.938	0.926	0.91	0.9

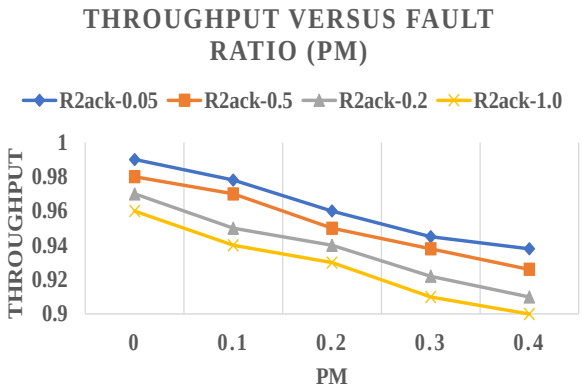

Fig. 4 Throughput versus fault ratio (Pm)

"As the number of nodes in a MANET network increases, the 2ACK time will also increase. This is seen in Figure 5. The algorithm selects a node randomly, and the wait time is 20 milliseconds. To calculate the time for the 2ACK packet, If a 2ACK is successfully received, it takes 20 milliseconds for it to be considered successful. If this is not the case, it is referred to as a "2ACK loss." Any time a node drops a packet, it poses a significant danger to the security of MANETs. The study is primarily concerned with packet loss, misbehaving nodes, and the overall impact on network performance. The cluster head is based on the energy of the nodes whenever packets are dropped, and the proposal uses the CEMCA algorithm in this study.

Table 6. Number of nodes versus time taken to acknowledge

Nodes	Time Taken to Acknowledge
5	2.5
10	6
20	8
30	12
40	14
50	17.5
60	21
70	23
80	26
90	31

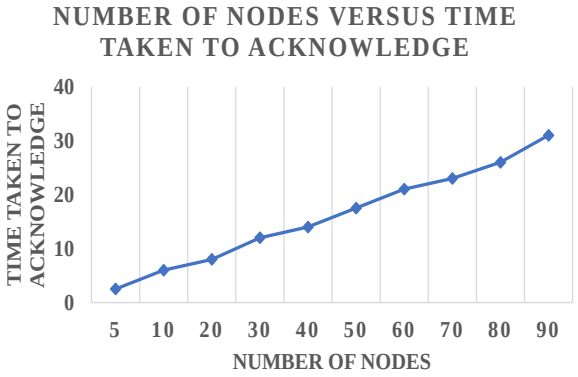

Fig. 5 Number of nodes versus time taken to acknowledge

Figure 6 depicts the number of packets that were transmitted and the number of 2ACKs that were missed. (Cpkts). The number of misbehaving nodes affects Cmiss because it determines how long it takes for each node to send two acknowledgments. Consequently, the graph depicts a wide range of diverse phenomena.

The cluster head requests a trust function from all the cluster nodes. Nodes may communicate misleading trust values about their nearby nodes, and if the cluster head determines that node to be a selfish node, data will be lost due to the decision.

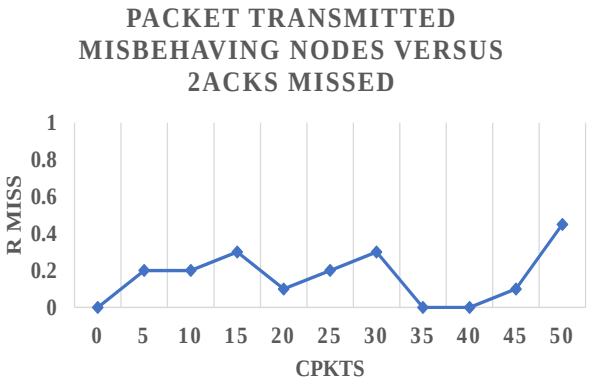

Fig. 6 Packet transmitted misbehaving nodes versus 2ACKs missed.

Table 7. Packet transmitted misbehaving nodes versus 2ACKs missed

Misbehaving Nodes	R-Miss
0	0
5	0.2
10	0.2
15	0.3
20	0.1
25	0.2
30	0.3
35	0
40	0
45	0.1
50	0.45

As a result, Tables 2, 3, 4, 5, 6, and 7 employ the 2ack technique to pinpoint the offending node; afterward, the cluster head determines whether or not a node is being selfish. To choose cluster heads in future work, need to use a different clustering technique. It is necessary to keep the overhead on the cluster head to a minimum. The findings of the simulation have been improved. Enhanced2ACKs are preferable to one than 2ACK.

6. Conclusion

MANETs (Mobile Ad hoc Networks) have been an increasingly popular research topic due to their potential use in military and civil communication networks. As the name implies, a mesh network is a networking infrastructure that relies heavily on all members' cooperation to carry out networking tasks effectively. Therefore, nodes that are self-serving or suffering difficulties are susceptible to it. Selfish (misbehaving) nodes and the performance damage MANET bring to the rest of the network are discussed in this article. A technique known as 2ACK has been created and tested to discover and mitigate the repercussions of a routing problem to improve network performance. There has been thorough research carried out on the usefulness of the 2ACK approach. 2ACK checks for message secrecy by comparing the hash code. The message's source with the hash code produced at the destination. Also, a security feature is included in the protocol as part of the proposed overall security strategy. Simulation findings demonstrate that the 2ACK technique can sustain a packet delivery ratio of up to 91 percent under certain situations, even when only 40 percent of the tested nodes in the MANETs are active. According to the results, the standard DSR technique could only transfer 40 percent of the packets it received. A significant focus is also placed on the false alarm rate and routing complexity of the 2ACK system. Using the R2ack option in the 2ACK method makes it possible to minimize overhead while still retaining performance.

References

[1] D. K. Mishra, “Tutorial: Privacy Preservation in Manet: Issues and Challenges," *2012 Third International Conference on Intelligent Systems Modelling and Simulation*, Kota Kinabalu, Malaysia, pp. 13-13, 2012.

[2] Jianguo Hao, Weidong Liu, and Yiqi Dai, “A Controllable Privacy Protection Framework in Position-Based Routing for Suspicious Manets," *Iet International Conference on Wireless Sensor Network* 2010 (Iet-Wsn 2010), Beijing, pp. 291-296, 2010.

[3] B. Kasiri, I. Lambadaris, F. R. Yu and H. Tang, “Privacy-Preserving Distributed Cooperative Spectrum Sensing in Multi-Channel Cognitive Radio Manets," *2015 Ieee International Conference on Communications (Icc)*, London, Uk, pp. 7316-7321, 2015.

[4] S. Joshi, R. Sheikh and D. K. Mishra, “Schematize Trust Overlays and Management for Privacy Preservation in Manet," *2010 Second International Conference on Computational Intelligence, Modelling and Simulation*, Bali, Indonesia, pp. 106-110, 2010.

[5] R. Sheikh, Mahakal Singh Chande and D. K. Mishra, “Security Issues in Manet: A Review," *2010 Seventh International Conference on Wireless and Optical Communications Networks - (Wocn)*, Colombo, Sri Lanka, pp. 1-4, 2010.

[6] S. A. Abbad and S. P. Godse, “Priority Based Emergency Message Forwarding Scheme for Time Critical Models in Vanet," *2016 Ieee International Conference on Advances in Electronics, Communication and Computer Technology (Icaecct)*, Pune, India, 393-398, 2016.

[7] M V Narayana, Aparnarajesh Atmakuri “A-Zhls: Adaptive Zhls Routing Protocol for Heterogeneous Mobile Adhoc Networks” *International Journal of Engineering & Technology*, vol.7, no.3, pp.1626- 1630, 2018.

[8] S. Joshi and D. K. Mishra, “A Roadmap Towards Trust Management & Privacy Preservation in Mobile Ad Hoc Networks," *2016 International Conference on Ict in Business Industry & Government (Ictbig)*, Indore, India, pp. 1-6, 2016.

[9] H. Kadhim and M. A. Hatem, “Secure Data Packet in Manet Based Chaos-Modified Aes Algorithm," *2019 2nd International Conference on Engineering Technology and Its Applications (Iiceta)*, Al-Najef, Iraq, pp. 208-213, 2019.

[10] A. El Hibaoui and L. Vallet, “Hypergraph Model for Anonymous Communications," *2012 International Conference on Multimedia Computing and Systems, Tangiers*, Morocco, pp. 888-894, 2012.

[11] M V Narayana, Rishi Sayal, H.S. Saini, Aparna Manikonda “Timestamp Based Certified Routing for Authorization and Authentication in Mobile Ad Hoc Network” *Journal of Advanced Research in Dynamical and Control Systems*, vol.10, no.10,pp. 351-358.

[12] R. Barskar, M. Ahirwar and R. Vishwakarma, "Secure Key Management in Vehicular Ad-Hoc Network: A Review," *2016 International Conference on Signal Processing, Communication, Power and Embedded System* (Scopes), Paralakhemundi, India, pp.1688-1694, 2016.

[13] Kim, M.; Jang, I.; Choo, S.; Koo, J.; Pack, S, "Collaborative Security Attack Detection in Software-Defined Vehicular Networks," *in Proceedings of the 2017 19th Asia-Pacific Network Operations and Management Symposium (Apnoms),* Seoul, Korea, pp. 19–24, 2017.

[14] Liu, Kejun, Et Al, "an Acknowledgment-Based Approach for the Detection of Routing Misbehavior in Manets," *Ieee Transactions on Mobile Computing*, vol.6, no.5, pp.536-550, 2007.

[15] Boopathi, G. Muruga, N. Insozhan, and S. Vinod, "Selfish Nodes Detection Using Random 2ack in Manet's," *Ijese,* vol.1, no.4 , pp.3-5, 2013.

[16] Kyasanur, P.; Vaidya, N.H, "Selfish Mac Layer Misbehavior in Wireless Networks," Ieee Trans. Mob. Comput, vol. 4, 502–516, 2005. [Crossref]

[17] Guang, L.; Assi, C, "Mac Layer Misbehavior in Ad Hoc Networks," *in Proceedings of the Canadian Conference on Electrical and Computer Engineering,* Saskatoon, Sk, Canada 1–4 May 2005; pp. 1103–1106. [Crossref]

[18] Silva, B.M.C.; Rodrigues, J.J.P.C.; Kumar, N.; Han, G, "Cooperative Strategies for Challenged Networks and Applications: A Survey, " *Ieee Syst. J.* vol.11, pp. 2749–2760, 2017. [Crossref]

[19] "Inet Framework Development Team. Inet Framework," 2020. Available Online: Https://Inet.Omnetpp.Org/ (Accessed on 13 November 2020).

[20] Vij, A.; Sharma, V. Nand, P, " Selfish Node Detection Using Game Theory in Manet," *in Proceedings of the 2018 International Conference on Advances in Computing, Communication Control and Networking (Icacccn),* Greater Noida (Up), India, pp. 104–109, 2018.[Crossref]

[21] Babu, S. Dilli, and Rajendra Pamula, "an Effective Block-Chain Based Authentication Technique for Cloud Based Iot," *International Conference on Advances in Computing and Data Sciences*, Springer, Singapore, 2020.

[22] Salvakkam, Dilli Babu, and Rajendra Pamula, "Messb–Lwe: Multi-Extractable Somewhere Statistically Binding and Learning with Error-Based Integrity and Authentication for Cloud Storage," *the Journal of Supercomputing,* pp.1-30, 2022.

[23] Salvakkam, Dilli Babu, and Rajendra Pamula, "Design of Fully Homomorphic Multikey Encryption Scheme for Secured Cloud Access and Storage Environment," *Journal of Intelligent Information Systems*, pp.1-23, 2022.

[24] Lupia, A.; Rango, F.D, "A Probabilistic Energy-Efficient Approach for Monitoring and Detecting Malicious/Selfish Nodes in Mobile Ad-Hoc Networks," *in Proceedings of the 2016 Ieee Wireless Communications and Networking Conference*, Doha, Qatar, pp. 1–6, 2016.

[25] Roselinmary, S.; Maheshwari, M.; Thamaraiselvan, M, "Early Detection of Dos Attacks in Vanet Using Attacked Packet Detection Algorithm (Apda)," *in Proceedings of the 2013 International Conference on Information Communication and Embedded Systems (Icices),* Chennai, India, pp. 237–240, 2013.

[26] Singh, A.; Sharma, P, "A Novel Mechanism for Detecting Dos Attack in Vanet Using Enhanced Attacked Packet Detection Algorithm (Eapda)," *in Proceedings of the 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (Raecs),* Chandigarh, India, pp. 1–5, 2015.

[27] Ilavendhan, A.; Saruladha, K, "Comparative Analysis of Various Approaches for Dos Attack Detection in Vanets," *in Proceedings of the 2020 International Conference on Electronics and Sustainable Communication Systems* (Icesc), Coimbatore, India, pp. 821–825, 2020.

[28] Wu, C.; Gerla, M.; Van Der Schaar, M, "Social Norm Incentives for Network Coding in Manets," *Ieee/Acm Trans. Netw*. vol.25, pp.1761–1774, 2017.

[29] Buttyán, L.; Hubaux, J.P, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *Mobile Netw. Appl.* vol. 8, pp.579–592, 2003. [Crossref]

[30] Meeran, A, "Enhanced System for Selfish Node Revival Based on Watchdog Mechanism*," in Proceedings of the 2017 International Conference on Trends in Electronics and Informatics (Icei),* Tirunelveli, India, 11–12 May 2017; P. 6.

[31] Li, Z.; Shen, H, "Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks," Ieee *Trans. Mob. Comput,* vol.11,pp.1287–1303, 2012. [Crossref]

[32] Khan, B.U.I.; Anwar, F.; Olanrewaju, R.F.; Pampori, B.R.; Mir, R.N, "A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission with Optimized Network Operations in Futuristic Mobile Adhoc Networks," *Ieee Access,* vol.8, pp.124097–124109, 2020.[Crossref]

[33] Yang, F.; Yan, J.; Guo, Y.; Luo, X, "Stackelberg-Game-Based Mechanism for Opportunistic Data Offloading Using Moving Vehicles," *Ieee Access*, vol.7, pp.66435–166450, 2019. [Crossref]

[34] Al-Terri, D.; Otrok, H.; Barada, H.; Al-Qutayri, M.; Al Hammadi, Y, "Cooperative Based Tit-for-Tat Strategies to Retaliate Against Greedy Behavior in Vanets," *Comput. Commun,vol*.104, pp.108–118, 2017.

[35] Xu, L.; Lin, Z.; Ye, A, "Analysis and Countermeasure of Selfish Node Problem in Mobile Ad Hoc Network," *in Proceedings of the 2006 10th International Conference on Computer Supported Cooperative Work in Design*, Nanjing, China, pp. 1–4, 2006. [Crossref]

[36] Kampitaki, D.G.; Karapistoli, E.D.; Economides, A.A, "Evaluating Selfishness Impact on Manets," *in Proceedings of the 2014 International Conference on Telecommunications and Multimedia (Temu)*, Heraklion, Crete, Greece, pp. 64–68, 2014. [Crossref]

[37] Loudari, S.E.; Benamar, N, "Effects of Selfishness on the Energy Consumption in Opportunistic Networks: A Performance Assessment," *in Proceedings of the 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (Wits)*, Fez, Morocco,pp. 1–7, 2019.

[38] Narayana, M. V., G. Narsimha, and S. S. V. N. Sarma, "Genetic-Zhls Routing Protocol for Fault Tolerance and Load Balancing," *Journal of Theoretical & Applied Information Technology*, vol. 83, no.1, 2016.

[39] Narayana, M. V., G. Narsimha, and S. S. V. N. Sarma, "Secure-Zhls: Secure Zone Based Hierarchical Link State Routing Protocol Using Digital Signature," *International Journal of Applied Engineering Research*, Issn (2015): 0973-4562, 2015.

[40] Sirisati, Ranga Swamy, Et Al, "an Energy-Efficient Pso-Based Cloud Scheduling Strategy," *Innovations in Computer Science and Engineering*, Springer, Singapore, pp.749-760, 2021.

[41] Narayana, M. V, "Route Optimization By Using Multiple Travelling Sales Person Problem in Manets," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol.3, no.1, pp.782-790, 2018.