CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-4, Issue-1 DOI: 10.46860/cgcijctr.2021.12.31.240

Trust-Based Security: Advancement towards Protection of the Ad-hoc Network

Samita Dhiman, Dr. Manish Kumar*
Department of Computer Science & Engineering,
Chandigarh Engineering College, Landran
Email Id: *manish.4379@cgc.edu.in

Abstract: **MANET (mobile ad hoc network) is a collection of mobile nodes that interact without the need for a fixed physical foundation. MANETs have grown in popularity as a result of characteristics like dynamic topology, quick setup, multi-hop data transfer, and so on. MANETs are well-suited to various real-time applications, including environmental monitoring, disaster management, and covert and military operations, because of their distinguishing characteristics. MANETs may also be used in conjunction with new technologies like cloud computing, IoT, and machine learning algorithms to help realize the vision of Industry 4.0. Secure and reliable data transfer is essential for any MANET-based sensitive real-time applications that must achieve the requisite QoS. It is challenging to provide safe and efficient data transfer with MANET. As a result, this article examines different Trust-based Approaches that take a step forward in providing secure transmission while simultaneously improving MANET performance. Furthermore, the study's analysis based on many aspects exposes the inadequacies of existing techniques and provides future directions for improvement.**

Indexed Terms: MANETs, Trust-based Security, Attacks, Analysis, PDR

I. INTRODUCTION

A Mobile Adhoc network is an infrastructure-free network made up of mobile nodes that dynamically choose the best path for data transmission. A MANET is a transitory network formed by mobile hosts with wireless network interfaces that do not require any fixed infrastructure or centralized administration. Nodes inside each other's wireless transmission ranges can interact directly, whereas nodes beyond the range must rely on other nodes to relay messages [1]. As a result, a multi-hop scenario arises, in which many intermediary hosts relay the packets transmitted by the source host before reaching the destination host. Each node serves as a router. The success of communication is strongly dependent on the cooperation of other nodes. Because of the mobility of the nodes, their transmitter/receiver coverage patterns, transmission power levels, and co-channel interference levels, the system may be seen as a random graph at any given moment. As nodes relocate or modify their transmission and reception characteristics, the network architecture may change over time. As a result, a MANET has a number of distinguishing properties [2]:

- Resource constraints
- Dynamic topology
- Limited physical security
- No infrastructure

Military personnel relaying information for alertness on the field of battle, business associates exchanging data during a meet and greet, participants using laptop computers to take part in an immersive conference, and case of emergencies, disaster relief employees trying to coordinate attempts after a fire, storm, or earthquake are all examples of MANET's potential applications. Personal area and home networking, location-based services, and sensor networks are other potential uses [3]. For wired and wireless network communications, security is a must-have service. MANET's success is heavily reliant on whether or not its security can be trusted. On the other hand, the features of MANET present both problems and possibilities in terms of meeting security requirements, including secrecy, authentication, integrity, availability, access control, and non-repudiation. The primary goal of network security, whether wired or wireless, is to protect network resources from a variety of attacks, including denial of service (DOS) attacks, black hole attacks, Gray hole attacks, wormhole attacks, routing table overflow, and poisoning attacks, packet replication attacks, and packet modification attacks [4][5][6].

The concept of trust and reputation has recently been applied to the field of wireless communication networks to monitor varying node behavior and counter insider attacks. Reputation and trust are two powerful tools that can help you make better decisions in various situations. Trust-based security [7] is a novel technique of delivering security that does not rely on encryption. Trust is defined as the degree of trustworthiness of other nodes performing actions [8]. Wireless networks can employ trust and reputation management systems (TRMs) to help them make decisions. The nodes' trust is maintained by documenting a node's transactions with other nodes in the network, either directly or indirectly [9]. The record will be used to compute a trust value that will help sensor nodes deal with uncertainty about future actions of other nodes. When dealing with node misbehavior, trust-based techniques are quite beneficial. The challenge of dealing with ambiguity in decision-making is addressed by trust and reputation management systems that keep track of node behavior in the past [10]. If a node has a good reputation, it will be trusted, and packets will be routed to it; otherwise, it will be deemed unreliable. In our personal and professional lives, the terms "trust" and "reputation" are frequently employed. A person's reputation is built on prior acts, and it grows over time if he or she is continuously honest in their interactions. The same concept is used in trust and reputation-based systems: a well-known node is picked for communication in the area [11].

The paper's following part delves into various threats in mobile Ad-hoc networks, as well as current trust-based solutions. Furthermore, the primary goal of this study is to examine the influence of trust-based techniques on security;

CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-4, Issue-1 DOI: 10.46860/cgcijctr.2021.12.31.240

thus, the analysis is based on attacks and approaches, as well as the factors that the researchers examined before.

II. ATTACKS IN MOBILE ADHOC NETWORK

MANET is vulnerable to a wide range of attacks. Some assaults target general networks, while others target wireless networks, and yet others target MANETs specifically. Different criteria, such as the attackers' domain or the tactics employed in assaults, can classify these security attacks. The criteria shown in the figure below [12] can be used to classify security threats in MANET and other networks: internal or external, various protocol layers, stealthy or non-stealthy, cryptography, or non-cryptography.

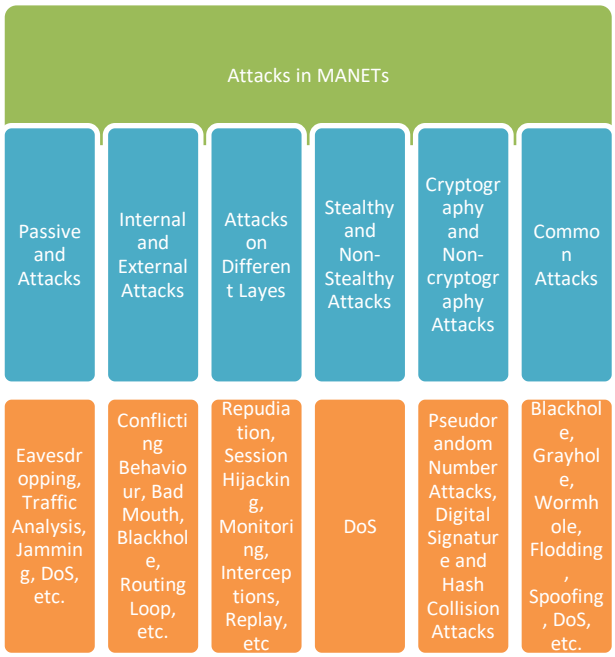

Fig 1: Different Categories of Attacks in MANETs

Passive and Active attacks: The assaults in MANET can be broadly divided into passive attacks and active attacks. A passive attack acquires data transmitted in the network without disturbing communications, but an active assault disrupts the regular operations by disrupting information interruption, alteration, or creation. Eavesdropping, traffic analysis, and traffic monitoring are examples of passive assaults. Jamming, impersonation, modification, denial of service (DoS), and message replay are examples of active assaults [13].

Internal and External attacks: According to the domain of the attacks, they may also be divided into external and inside attacks. Outsider and insider assaults are mentioned in several articles [14]. External assaults are carried out by nodes that are not part of the network's domain. Internal assaults are carried out by network nodes that have been hacked. Internal assaults are more severe than external attacks because the insider has access to sensitive information and has privileged access permissions.

Attacks on different layers: The assaults may be further categorized using the Internet model's five levels [15]. The following is a categorization of different security threats on each tier of the Internet model.

- Application layer- Repudiation, data corruption
- Transport layer- Session hijacking, SYN flooding
- Network layer- Wormhole, blackhole, flooding, etc
- Data link layer- Traffic analysis, monitoring, WEP weakness, disruption MAC (802.11)
- Physical layer- Jamming, eavesdropping, interceptions
- Multi-layer attacks - DoS, replay, man-in-the-middle

Stealthy and Non-stealthy attacks: Some security assaults employ stealth, in which the attackers attempt to conceal their activity from either a human observer or an intrusion detection system (IDS). However, other assaults, such as denial-of-service (DoS), cannot be made inconspicuous [16].

Cryptography and Non-cryptography attacks: Some of the assaults aren't linked to cryptography, while others are basic cryptographic attacks. The following are some examples of cryptographic primitive attacks:

- Pseudorandom number attack- Nonce, initialization vector, timestamp
- Digital signature attack- RSA signature, digital signature standard (DSS)
- Hash collision attack- SHA-0, MD4, MD5

Some commonly found Attacks in MANETs: Black hole, Wormhole, Gray hole, Rushing, Flooding, Spoofing, Denial of Service (DoS), and other assaults are widespread on the Mobile Ad-hoc Network [17]. These assaults fall under the above categories and have a significant impact on network performance.

III. TRUST-BASED SECURITY APPROACHES

This section describes different trust-based security techniques for Mobile Ad-hoc Networks developed to detect attackers or protect the network from them. The trust factor is influenced by a number of factors and can be calculated either directly or indirectly. The following are some of the trust-based MANET methods that have been proposed:

Security Trust Monitor (STM): Lacharité et al. [18] proposed a generic design for a routing protocol-based security trust monitoring layer. This security layer may be deployed to various MANET routing protocols and enable monitoring of various network threats by adding particular plug-ins. This modular security method enables nodes with different routing protocols and security solutions to communicate with one another by sharing security information. The goal is for a security layer to monitor MANET communication and build a trust representation model of MANET member nodes. On request, the trust information obtained may be sent to MANET nodes, who can then alter their routing tables accordingly. They also demonstrated that this security architecture could be tested on a genuine MANET. They used the integration of wormhole detection and countermeasures with the security trust monitoring layer conducted on the same test bed as an example of a security assault.

TAODV: In order to improve the performance of MANETs, Balakrishna et al. [19] suggested Trust based AODV (TAODV). TAODV employs trust measurements to improve routing decisions and punish nodes that refuse to cooperate. These measurements included the time it takes a node to create, process, and update RREP and R ACK messages, as well as per-packet overhead. They also compared its performance to that of SAODV and discovered that it had improved.

Trust-based Optimal Routing (TRRP): In MANETs, Neelakandan and Anand [20] presented a safe, trustworthy, and optimum routing system. This research aims to provide an attack detection and protection mechanism based on route redundancy in ad hoc networks and message redundancy in routing protocol topology discovery. Both trustworthiness and performance are combined in the best routing method. As a result, this was the first safe routing system that took into account the detection of tough internal assaults and network performance. The simulation results showed that the suggested attack detection algorithm and optimum routing protocol are effective and superior to well-known protocols like AODV.

Threshold-based Trust Counter (TTC): Sharma et al. [21] devised a trust-based packet forwarding method based on routing layer information for identifying and isolating rogue nodes. Each node kept a trusted counter, which was increased and decremented based on punishment and rewards. If the value of this counter goes below the threshold, the node is considered malicious.

Multi-dimensional trust management scheme (M-TMS): For MANETs, Li et al. [22] presented a collaborative and trust-based outlier identification method that considers a node's reputation. With a low communication cost, the method produces a shared outlier view among dispersed nodes. The suggested approach is efficient and accurate, according to simulation findings.

Secure Trusted Route Selection (STRS): For a trusted route selection value, Gupta et al. [23] suggested a secure gateway based on node trust values, route trust values, and residual route load capacity. They also focused on the authentication procedure for mobile nodes and secure gateways using a pre-authentication approach. It's crucial to assess a safe, trusted route to the secure gateway and verify the mobile node and secure gateway to offer host-to-host security. The suggested method was successful in achieving this goal. When compared to existing protocols, the suggested protocol performs better. Simulation data and performance assessment matrices were used to verify the accuracy of the suggested strategy.

Trust-Based Secure on Demand Routing Protocol (TSDRP): TSDRP is a Trust-Based Secure on Demand Routing Protocol developed by Aggarwal et al. [24]. TSDRP has been added to the Ad hoc On-Demand Distance Vector (AODV) routing protocol to make it safe against attacks such as Blackhole and DoS assaults. They used Packet Delivery Fraction (PDF), Average Throughput (AT), and Normalized Routing Load to assess the performance (NRL).

Clustering-based Trust Evaluation (CTE): To minimize Vampire and DDoS assaults, Dangare and Mangrulkar [25] developed a trust-based strategy. They employed clustering, taking into account ten nodes in a cluster and selecting the two nodes with the most energy to serve as cluster heads. They also employed counting how many packets a node sends and receives and comparing it to a threshold number. The outcomes demonstrated the advantages of the recommended strategy.

Trust-based Power-Aware DSR routing protocol (FTP-DSR): Jayalakshmi and Razak [26] presented a unique trust-based power-aware routing method that selects the most trustworthy path using fuzzy logic prediction criteria. This approach produces a route that includes nodes with high trusted values and eliminates nodes with low remaining battery power. The suggested model was included in the widely used DSR routing protocol. The Trust-based Power-Aware DSR routing protocol (FTP-DSR), a unique on-demand trust-based source routing protocol for MANETs, offered a flexible and viable way for choosing the route that fulfills the security requirements of data packet transmission. Experiments have been carried out to assess the efficiency and efficacy of the proposed approach in detecting rogue nodes and defending against attacks. Compared to normal DSR routing, the findings demonstrated that FTP-DSR improves the packet delivery ratio and reduces average end-to-end latency.

Trust-based Certificate Revocation for Secure Routing (TCRSR): To decrease node risks and improve network security, Rajkumar and Narsimha [27] suggested a CA distribution and Trust-based threshold revocation technique. The trust value was first calculated using the direct and indirect trust values. The secret key was disseminated to all nodes by the certificate authority. After that, a trust-based threshold revocation procedure was calculated, and the offending nodes were removed.

Trust-Based Authenticated Anonymous Secure Routing (TBASR): TBASR was proposed by Jain et al. [28] for MANET in a hostile environment. This protocol protects against neighbor node attacks by encrypting and decrypting keys through route-request and reply. Group signature was used to establish node trust, while asymmetric key encryption was used to establish path trust. It identifies intruders in networks and eliminates traffic delays between opponent nodes by doing so. During packet transmission, onion routing is utilized to maintain anonymity.

Secure and Trust-based AODV (STAODV): STAODV was suggested by Kamel et al. [29] to increase the security of the AODV routing protocol. The method identifies hostile nodes who attempt to attack the network based on their primary data. Each participating node was assigned a trust level to determine its level of trust. To avoid a black hole attack, each incoming packet was inspected.

Trust-Based Secure and QoS Routing Strategy (TSQRS): By integrating social and QoS trust, Pathan et al. [30] presented a trust-based secure QoS routing system. The proposed scheme's principal strategy is to mitigate nodes that display various packet forwarding misbehavior and identify the path that provides reliable communication via the trust mechanism. The method will choose the optimal forwarding node based on packet forwarding behavior and QoS factors, including residual energy, channel quality, and connection quality, among others. They created an adversary model for packet-dropping attacks against which the suggested method was tested. In terms of overhead, packet delivery ratio, and energy consumption, a simulation experiment utilizing Network Simulator-2 (NS2) and various network conditions show

that combining social and QoS trust factors may substantially enhance the security and quality of service routing.

TSD Secure Algorithm: Bharati [31] proposed trust computation protocols and a TSD algorithm that determined the secure shortest routes. Trust is one of the ways to enhance the security of MANETs, so this paper contributed to enhancing the security of MANETs by fusing the trust in the TSD algorithm. The algorithm is described, and its performance is measured, compared, and validated. The algorithm is superior because it considers both shortest distances and computed trust values of nodes in route findings.

Dual Attack Detection for the black and gray hole (DDBG): For MANETs, Zardari et al. [8] introduced a popular approach known as dual attack detection for black and grey hole assaults (DDBG). The proposed DDBG approach uses the connected dominant set (CDS) technique with two extra features: the energy and the node's absence from the blacklist are also verified before adding it to the IDS set. In mobile ad hoc networks, the CDS is an effective, distinct, and confined method for finding nearly-connected dominant groups of nodes in a short region. To obtain the full behavioral information from their nodes, the selected IDS nodes broadcast a sort of status packet inside the size of the dominant set. Later, IDS nodes utilize the DDBG method to evaluate the gathered behavioral data to identify malicious nodes and add them to the blacklist if their behavior is suspicious. The experimental findings demonstrate that the suggested approach surpasses existing routing strategies in terms of service parameters quality.

Secure Detection Prevention and Elimination Gray Hole (SDPEGH): SDPEGH is a method suggested by Radha and Rao [32] for detecting, preventing, and eliminating the grey hole malicious node that participates in route finding. The proposed and current systems' performance parameters, such as PDR, throughput, security, and energy usage, were examined. The suggested system's performance is superior to the other approaches.

Trust-Based Efficient Blockchain Linked Routing Method (TbEBCLRM):A system comprising trustworthy and untrusted nodes, Narayana and Chakkaravarthy [33] suggested a TbEBCLRM. The proposed technique used blockchain technology to increase security in ad hoc networks and prevent harmful actions from taking place during communication. The suggested approach was compared to existing methods, with the findings indicating that the new method outperforms the traditional methods in terms of accuracy, security, trust, and energy usage.

Trust-Based Secure Multipath Routing Protocol (TBSMR): To improve the MANET's overall performance, Sirajuddin et al. [34] introduced TBSMR, a trust-based multipath routing protocol. The proposed protocol's major strength was that it considered different aspects to improve the MANET's QoS, such as congestion control, packet loss reduction, malicious node identification, and secure data transfer. A simulation in NS2 was used to evaluate the suggested protocol's performance. The simulation results show that the proposed routing protocol outperforms existing methods.

The table1 below shows the existing trust-based methods and the parameters they took into account in their research. This contains information about the basic protocol, the performed attacks, the simulator that was used, the number of normal and attacker nodes, and performance metrics. Varied studies presented their results with different settings, but the table generally displayed the suggested protocol's packet delivery ratio (PDR), which is the most important performance metric for any network.

IV. REVIEW ANALYSIS

This suggested study's major goal is to examine the trust-based techniques created for Mobile Ad-hoc Networks. This section assessed existing research based on several characteristics such as Protocol, Attack, Simulator, Node-Attack Ratio, and performance metrics. All of the available methods are depicted in Table 1.

Adhoc Protocols: As shown in the following diagram, most current methods were examined for AODV-based MANETs. These findings are assessed only based on this investigation.

According to the graph above, the researchers viewed OLSR and DSDV protocols as a minimum, while 11 percent considered DSR, and up to 55 percent chose AODV as their basic procedure. This is primarily due to the AODV protocol's popularity and advantages over competing protocols. Even though it is extremely vulnerable to a variety of assaults.

Simulator Used: The NS-2 Simulator was used for the bulk of the simulations, as shown in the diagram below. As a result, NS-2 is the most widely used simulator for examining Mobile Ad-hoc Network Protocols and Algorithms. It will continue to be utilized in the future
Other simulators, such as Glomosim, are also used by a small number of researchers, as seen in the graph above. Furthermore, only 10% of the works conducted real-time testing of the recommended techniques. Because real-time systems are accurate testers, the methods may be put to the test in a real-time or real-test bed environment to reveal the actual performance of the suggested algorithms/ protocols.

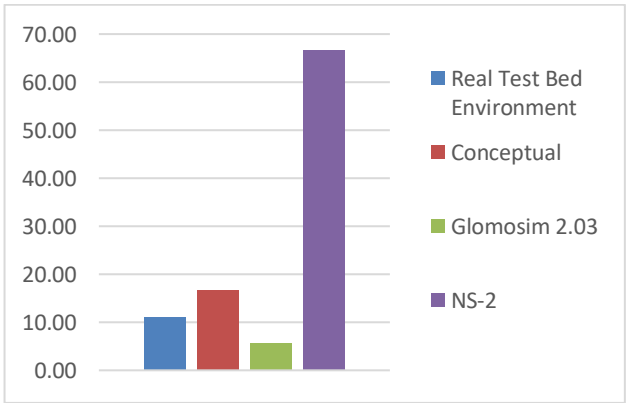

Fig 2: Simulator Used in the Existed Systems

Different Attacks and Node-Attack Ratio: This investigation also discovered the assaults that the researchers examined while evaluating their techniques. The pie chart below depicts the proportion of various assaults evaluated by various scholars.

Table 1: Existing Trust based Approaches in MANETs

Author Name	Year	Approach Name	Protocol	Attack	Simulator	Number of Nodes	Number of Attacker Nodes	Results
Lacharité et al. [18]	2008	STM	OLSR	Wormhole	Real Test Bed Environment	10	2	Successfully detects an attacker as a false node
Balakrishna et al. [19]	2010	TAODV	AODV	-	Real Systems	5	-	RTT-172.553
Neelakandan and Anand [20]	2011	TRRP	AODV	Packet Drop Attack	NS-2	50	5,10,20	Max PDR is nearly 80%
Sharma et al. [21]	2011	TTC	AODV	-	Conceptual	-	-	Reduces Security Threats
Li et al.[22]	2012	M-TMS	-	DoS	GloMoSim 2.03	50, 100, 150, 200	5,10,20	With 20 malicious nodes, CR is more than 80%
Gupta et al. [23]	2014	STRS	-	-	NS-2	-	-	Average PDR increases by 3.6%
Aggarwal et al. [24]	2014	TSDRP	AODV	Black hole and DoS	NS-2	70	0-7	More than 80% PDR
Dangare and Mangrulkar [25]	2015	CTE	AODV	Vampire and DDoS	NS-2	30	-	Improved performance
Jayalakshmi and Razak [26]	2016	FTP-DSR	DSR	malicious nodes and selfish nodes	NS-2	25	0-10	More than 70% PDR
Rajkumar and Narsimha [27]	2016	TCRSR	DSR		NS-2	50	-	PDR-up to 96%
Jain et al. [28]	2017	TBASR	-	-	Conceptual	-	-	ensures the secure and trusted communication
Kamel et al. [29]	2017	STAODV	AODV	Black hole	NS-2	25	1-4	PDR: 97-98%
Pathan et al. [30]	2018	TSQRS	AODV	Gray hole	NS-2	50	0-40%	Min PDR 60% in presence of 40% malicious nodes (Max PDR-80%)
Bharati [31]	2019	Secure TSD	-	-	Conceptual	-	-	Better Algorithm
Zardari et al.	2019	DDBG	AODV	Black	NS-2	100	-	PDR: 95-

[35]				and Gray hole				97%
Radha and Rao [32]	2019	SDPEGH	DSDV	Gray Hole	NS-2	45	-	PDR: 48%
Narayana and Chakkaravarthy [36]	2020	TbEBCLRM	AODV	-	NS-2	50, 100, 150, 200	-	PDR: 75-80%
Sirajuddin et al. [34]	2021	TBSMR	AODV	-	NS-2	50, 100, 300	-	Max PDR: 98%

scholars.

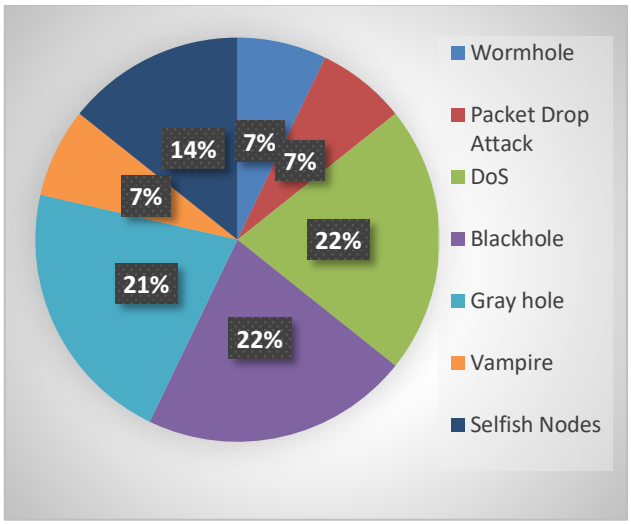

Fig 3: Different Attacks used for Analysis

According to the Figure 3, most studies concentrated on Black hole, DoS, and Gray hole assaults. These assaults have a significant impact on performance and degrade it in terms of several aspects. The node-attack ratio considered in existing trust-based simulations is depicted in the diagram below.

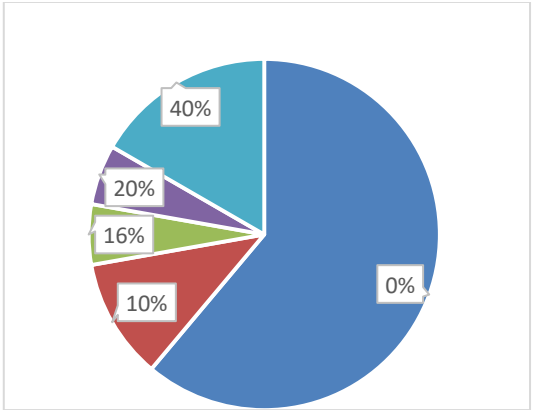

Fig 4: Node-Attack Ratio

The figure 4 shows that the majority of the recommended techniques were not tested with attacker nodes, according to the study's evaluation. As a result, the efficiency of existing methods cannot be justified. This also paves the way for future performance testing of existing protocols with attacker nodes.

Performance Measure: The Packet Delivery Ratio (PDR) is the most frequent and essential performance measure that researchers evaluate when evaluating their results. In the figure 5, the PDR of some of the existing protocols is shown.

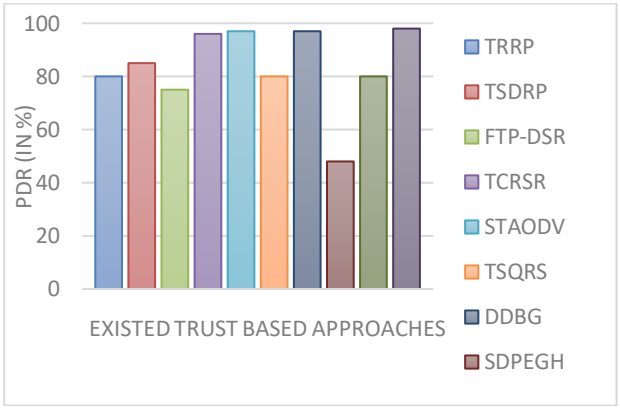

Fig 5: PDR of Existed Trust based Approaches

In terms of PDR, the figure above depicts the results obtained by various techniques. As mentioned in the preceding section, the majority of the protocols were tested without an attacker node; thus, a greater PDR seems dubious and should be investigated further to confirm the results.

V. CONCLUSION

This research indicates that trust-based techniques enhance the Ad-hoc Network in terms of intruder detection and prevention. Any of the stated categories in section 2 can be used to describe the invader. This research also assessed the work done based on criteria such as protocol selection; assaults examined, simulator utilized, Node-attack ratio, Performance Measurement, and future aspects of the Mobile Ad-hoc Network. The study's key conclusions suggest that existing protocols must be assessed in the face of highly susceptible assaults such as a black hole, grey hole, and DoS, with a changing ratio of attackers, for performance validation. Another finding claims that researchers may use the NS-2 Simulator to evaluate their suggested approaches because researchers extensively use it. Furthermore, the study might be expanded to include attacks, their ratios, other protocols, and various performance metrics.

REFERENCES

[1] C. E. Perkins, "Perkins, Ad Hoc Networking | Pearson," 2001. https://www.pearson.com/uk/educators/higher-

education-educators/program/Perkins-Ad-Hoc-Networking/PGM406134.html (accessed Jul. 25, 2021).

[2] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wirel. Commun., vol. 11, no. 1, pp. 38–47, Feb. 2004, doi: 10.1109/MWC.2004.1269716.

[3] V. Tsetsos, G. Alyfantis, T. Hasiotis, O. Sekkas, and S. Hadjiefthymiades, "Towards Commercial Wireless Sensor Networks: Business and Technology Architecture," Semant. Sch., vol. 2, pp. 59–80, 2006.

[4] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," Int. J. Comput. Sci. Inf. Secur. IJCSIS, vol. 4, no. 1 & 2, pp. 1–9, 2009.

[5] A. Jain, K. Kant, and M. . Tripathy, "Security Solutions for Wireless Sensor Networks," in 2012 Second International Conference on Advanced Computing & Communication Technologies, Jan. 2012, pp. 430–433, doi: 10.1109/ACCT.2012.102.

[6] Z. Zhou and C. Yow K, "Geographic ad hoc routing security: attacks and countermeasures.," Ad Hoc Sens. Wirel. Networks, 2005, 1(3) 235–253, vol. 1, no. 3, pp. 235–253, 2005.

[7] S. Devisri and C. Balasubramaniam, "Secure Routing Using Trust Based Mechaniam in Wireless Sensor Networks(WSNs)," Int. J. Sci. Eng. Res., vol. 4, no. 2, 2013.

[8] S. Sahil Babu, "LSR Protocol Based on Nodes Potentiality in Trust and Residual Energy for WSNs," Int. J. Netw. Secur. Its Appl., vol. 4, no. 2, pp. 21–34, 2012, doi: 10.5121/ijnsa.2012.4202.

[9] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 867–880, May 2012, doi: 10.1016/j.jnca.2011.03.005.

[10] J.-H. Cho, A. Swami, and I.-R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE Commun. Surv. Tutorials, vol. 13, no. 4, pp. 562–583, 2011, doi: 10.1109/SURV.2011.092110.00088.

[11] A. Ahmed, K. Abu Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," Front. Comput. Sci., vol. 9, no. 2, pp. 280–296, 2015, doi: 10.1007/s11704-014-4212-5.

[12] B. Wu, J. Chen, J. Wu, and M. Cardei, "A SURVEY OF ATTACKS AND COUNTERMEASURES IN MOBILE AD HOC NETWORKS," Mem. Detect. Theory Appl. Concealed Inf. Test, pp. 103–135, 2011, doi: 10.1017/CBO9780511975196.012.

[13] U. Ahamed and S. Fernando, "Identifying the Impacts of Active and Passive Attacks on Network Layer in a Mobile Ad-hoc Network: A Simulation Perspective," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 11, pp. 600–605, 2020, doi: 10.14569/IJACSA.2020.0111173.

[14] V. Divya and R. Gobinath, "ROUTING PROTOCOL AND SECURITY THREATS IN MANET," Int. J. Sci. Technol. Res., vol. 9, no. 04, pp. 799–802, 2020.

[15] C. V. Raghavendran, G. N. Satish, and P. S. Varma, "Security Challenges and Attacks in Mobile Ad Hoc Networks," Int. J. Inf. Eng. Electron. Bus., vol. 5, no. 3, pp. 49–58, 2013, doi: 10.5815/ijieeb.2013.03.06.

[16] T. Sui, Y. Mo, D. Marelli, X. Sun, and M. Fu, "The Vulnerability of Cyber-Physical System under Stealthy Attacks," IEEE Trans. Automat. Contr., vol. 66, no. 2, pp. 637–650, 2021, doi: 10.1109/TAC.2020.2987307.

[17] M. Sharma and M. Rashid, "Security Attacks In MANET – A Comprehensive Study," SSRN Electron. J., no. April, 2020, doi: 10.2139/ssrn.3565860.

[18] Y. Lacharité, D. Q. Nguyen, M. Wang, and L. Lamont, "A trust-based security architecture for tactical MANETs," Proc. - IEEE Mil. Commun. Conf. MILCOM, no. December 2008, pp. 1–8, 2008, doi: 10.1109/MILCOM.2008.4753215.

[19] R. Balakrishna, U. R. Rao, and G. A. Ramachandra, "Trust-based Routing Security in MANETS," IJCSE) Int. J. Comput. Sci. Eng., vol. 02, no. 03, pp. 547–553, 2010.

[20] S. Neelakandan and J. Gokul Anand, "Trust based optimal routing in MANET's," 2011 Int. Conf. Emerg. Trends Electr. Comput. Technol. ICETECT 2011, pp. 1150–1156, 2011, doi: 10.1109/ICETECT.2011.5760293.

[21] S. Sharma, R. Mishra, and I. Kaur, "New Trust Based Security Approach for Ad-HOC Networks," J. Mob. Commun., vol. 5, no. 1, pp. 1–5, 2011.

[22] W. Li, J. Parker, and A. Joshi, "Security through collaboration and trust in MANETs," Mob. Networks Appl., vol. 17, no. 3, pp. 342–352, 2012, doi: 10.1007/s11036-010-0243-9.

[23] A. K. Gupta, R. Kumar, and N. K. Gupta, "A trust based secure gateway selection and authentication scheme in MANET," Proc. 2014 Int. Conf. Contemp. Comput. Informatics, IC3I 2014, pp. 1087–1093, 2014, doi: 10.1109/IC3I.2014.7019816.

[24] A. Aggarwal, S. Gandhi, N. Chaubey, and K. A. Jani, "Trust based secure on demand routing protocol (TSDRP) for MANETs," Int. Conf. Adv. Comput. Commun. Technol. ACCT, pp. 432–438, 2014, doi: 10.1109/ACCT.2014.95.

[25] N. N. Dangare and R. S. Mangrulkar, "Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc Network," Phys. Procedia, vol. 78, pp. 342–349, 2016, doi: 10.1016/j.procs.2016.02.070.

[26] V. Jayalakshmi and T. Abdul Razak, "Trust based power aware secure source routing protocol using fuzzy logic for mobile adhoc networks," IAENG Int. J. Comput. Sci., vol. 43, no. 1, pp. 98–107, 2016.

[27] B. Rajkumar and G. Narsimha, "Trust Based Certificate Revocation for Secure Routing in MANET," Procedia Comput. Sci., vol. 92, pp. 431–441, 2016, doi: 10.1016/j.procs.2016.07.334.

[28] S. Jain, N. M. J. Kumari, and R. V, "Trust Based Authenticated Anonymous Secure Routing For MANET," ResearchGate, vol. 2, no. 5, pp. 41–46, 2020.

[29] M. B. M. Kamel, I. Alameri, and A. N. Onaizah, "STAODV: A secure and trust based approach to mitigate blackhole attack on AODV based MANET," in 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Mar. 2017, vol. 1, pp. 1278–1282, doi: 10.1109/IAEAC.2017.8054219.

[30] M. S. Pathan, Z. A. Zardari, and M. Q. Memon, "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs," Futur. Internet, vol. 10, no. 2, p. 16, Feb. 2018, doi: 10.3390/fi10020016.

[31] T. S. Bharati, "Trust based security of MANETS," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 8, pp. 792–795, 2019.

[32] M. Radha and M. Nagabhushana Rao, "Gray hole attack detection prevention and elimination using Sdpegh in manet," Int. J. Eng. Adv. Technol., vol. 8, no. 3, pp. 605–614, 2019.

[33] V. L. Narayana and D. Midhunchakkaravarthy, "A Trust Based Efficient Blockchain Linked Routing Method for Improving Security in Mobile Ad hoc Networks," Int. J. Saf. Secur. Eng., vol. 10, no. 4, pp. 509–516, 2020, doi: 10.18280/ijsse.100410.

[34] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/5521713.

[35] Z. A. Zardari et al., "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs," Futur. Internet, vol. 11, no. 3, 2019, doi: 10.3390/fi11030061.

[36] A. K. Naveena and N. K. Narayanan, "Image retrieval using combination of color, texture and shape descriptor," 2016 Int. Conf. Next Gener. Intell. Syst. ICNGIS 2016, 2017, doi: 10.1109/ICNGIS.2016.7854023.

[37] Tripathi, K.N., Sharma, S.C. A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS). Int J Syst Assur Eng Manag 11, 426–440 (2020). https://doi.org/10.1007/s13198-019-00871-0