JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.12, December 2021 E-ISSN: 2347-2693

A Deep Study of Hybrid Trust Built To Improve Security Technique against Sybil Attack in MANET Based IoT Network

Prince Kumar [1*], Rachana kamble[2]

[1,2]M.Tech. Scholar of Computer Science & Engineering Technocrats Institute of Technology, Bhopal, India

Corresponding Author: princekumarr9@gmail.com

DOI: https://doi.org/10.26438/ijcse/v9i12.18 | Available online at: www.ijcseonline.org

Received: 07/Dec/2021, Accepted: 10/Dec/2021, Published: 31/Dec/2021

***Abstract*—** The location of the mobile nodes in the MANET IoT changes continuously that's why the communication among them is difficult. The different devices or nodes in the Internet of Things (IoT) connect with each other over the internet or convey information to each other if they are immediately in range. The existence of an attacker is a difficult issue in a network since it lowers routing performance and has an impact on node battery life. Secure routing is critical to the adoption and deployment of many IoT applications. Sybil attacks may be destructive to MANET IoT and constitute a significant problem for building effective IoT security solutions. In this dissertation, proposes the Hybrid trust based enhanced security technique to protect the MANET IoT network against Sybil Attack. The preceding Sec Trust method is recommended as a dependable approach in IoT to safeguard communication from Sybil attack. The proposed system also decreases energy usage, which increases network life time. The performance of both the schemes is measured in different node density situations, but Hybrid trust performs better. The Sec trust system is dependable and secure, but it is inefficient in routing between the source and destination. The efficient routing technique decreases network overhead, which reduces packet flooding and, as a result, improves routing efficiency. The Hybrid trust method enhances routing reliability by consuming the energy consumption of mobile nodes in an MANET IoT network.

***Keywords*—** IoT-MANET, Nodes, Hybrid Trust, Sec trust, Routing, Sybil Attacker

I. INTRODUCTION

To accomplish system functioning, a mobile network generally consists of heterogeneous nodes that execute peer-to-peer wireless communications. Mobile networks include mobile ad-hoc networks (MANETs) [1], delay/disruption tolerant networks (DTNs) [2], mobile wireless sensor networks (WSNs) [3], Internet of things (IoT) systems [4] etc. (The fundamental characteristics of mobile networks are reconfigurability (minimal infrastructure reliance), distributed control (no requirement for a centralized body to manage the network), and dynamicity (change of network topology, population size, etc.). Mobile networks have been widely used in a variety of civil and military applications due to these characteristics. Conference attendees, for example, can build up an ad-hoc network using their laptops for instant messaging and discussion without relying on any wireless infrastructure, such as access points or wireless routers. In a wartime situation, a commander can dynamically build and manage a mobile network of trusted group members in order to complete a crucial objective. Sensors are linked to wild animals in zoology studies to build a delay-tolerant WSN for tracking long-term animal migratory habits [5]. A node in a mobile network might be an autonomous or human-operated device that collaborates with others. Many assaults may be made against a mobile network. Mobile networks suffer additional mobility-induced assaults [6], such as black-hole, wormhole, Sybil, and slandering attacks, in addition to attacks on wireless networks such as eavesdropping, tampering, jamming, and denial of service attacks [7]. Insider attacks are difficult to resist with standard encryption approaches when a node in a mobile network is compromised. Because mobile networks typically lack a trustworthy third party, each participating node may be forced to judge the trustworthiness of others based on direct and/or indirect observations.

In this paper work are divided into subsection such as section I is a introduction about the routing strategy, section II is a related work in the field of multipath and multichannel strategy, section III is a methodology, section IV proposed algorithm, section V describe about proposed architecture, section VI describe result discussion, section VII is conclusion of our proposed work.

II. RELATED WORK

In this section discuss about what are the contribution by the IoT mobile ad hoc network communication researcher in the area of secure routing strategy, attack detection and prevention. Those work elaborate in the below.

Prakash Srivastava, Aditya Tandon [8] The Internet of Things (IoT) is an emerging technology that plays a critical role in interconnecting various objects into a network to provide desired services within its resource-constrained characteristics. In this title, we discuss “Trust-based

Enhanced Secure Routing against Rank and Sybil Attacks in IoT" The Routing Protocol for Low Power and Lossy Networks (RPL) is a standardized proactive routing protocol for the Internet of Things that achieves satisfactory resource usage while ignoring the node's routing behavior while forwarding data packets. Malicious attackers take use of these flaws to execute various types of routing attacks. For identifying these attacks individually, several security techniques have been implemented.
Ismail Butun, Member, IEEE, *et.al.* [9] "Vulnerabilities, Attacks, and Countermeasures in Internet of Things Security" Wireless Sensor Networks (WSNs) are one of the most promising technologies of the third millennium, with a wide range of applications in our everyday lives. The widespread use of WSNs in many applications is due to their many appealing characteristics, including as inexpensive production costs, low installation costs, unattended network operation, autonomy, and long-term operation. Through the development of Internet access capabilities in sensor nodes and sensing capability in Internet-connected devices, WSNs have begun to combine with the Internet of Things (IoT).

Wang, Yizhong [10] "Secure routing protocol over mobile Internet of Things wireless sensor networks" is a term used to describe a protocol that is used to route data securely. Due to its low cost and ease of deployment, a wireless Internet of Things (IoT) network is utilized for military operations; nevertheless, one of the major difficulties with IoT networks is their lack of coherent security and privacy standards. We successfully built and implemented a lightweight trust-based security algorithm to facilitate routing in a mobile IoT wireless sensor network for this thesis project. To ensure appropriate node authentication and protect against Denial-of-Service and Sybil-based identity attacks, the standard routing protocol for IoT, known as routing protocol for low power and lossy networks (RPL), was modified to include common security techniques, such as a nonce identity, timestamp, and network white list.

Ruchi Mehta, M.M.Parmar [11] "A Survey on Security Attacks and Countermeasures in RPL for Internet of Things" The Internet of Things is gaining a lot of attention in today's world and has become a part of everyday life, resulting in a wide scale of deployment of Low Power and Lossy Networks (LLN). These networks, which constitute a network of IoT devices, embedded sensors, and their linkage to the Internet, have been used in the worlds of home automation, industry, life sciences, agriculture, military, and others.

VISHAL SHARMA, (Member, IEEE), *et. al.* [12] "Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey" The Internet of Things (IoT) has attracted companies and academicians from all over the world due to its wide variety of applications. The Internet of Things (IoT) makes operations easier by offering Internet access to all devices with computer capability. The focus has changed from simple IoT to smart, connected, and mobile IoT (M-IoT) devices and platforms, which can allow low-complexity, low-cost, and efficient computing through sensors, machines, and even crowd sourcing, thanks to the growth of wireless infrastructure. M-IoT is a phrase that may be applied to all of these devices. Despite the beneficial impact on applications, security, privacy, and trust remain important problems for such networks, with poor enforcement of these standards posing significant dangers to M-IoT devices and platforms. Hassan I. Ahmed, Abdurrahman A [13] "A survey of IoT security threats and defenses" The Internet of Things (IoT) is a well-known term that refers to the connectivity of physical and virtual devices in order to exchange data. The Internet of Things (IoT) ecosystem may link billions of devices or items, each with its own unique ID for identifying purposes. The Internet of Things (IoT) is widely regarded as one of the most important technologies of recent decades, with applications in healthcare, manufacturing, agriculture, military applications, and space science.

WeidongFang, Wuxiong Zhang, *et.al.* [14] "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey" Information security in wireless sensor networks (WSNs) is essential as a major component of information sensing and aggregation for big data, cloud computing, and the Internet of Things (IoT). WSN is becoming a susceptible target for various security threats due to the sensor node's limited resources. Internal assaults are harder to fight against than external attacks. Encryption and authentication techniques can be used to protect the former. This isn't true for the latter, which has access to all of the network's keys. According to research, trust management technology is one of the most effective ways to identify and fight against internal assaults.

Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, *et. al.* [15] "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks" We examine various distinct forms of internal attacks directed at the Rank property in this book, as well as their influence on the wireless sensor network's performance. Our findings highlight the possibility of an RPL flaw, namely the lack of a monitoring parent in each node. In RPL, the child node only receives parent information via control messages and is unable to inspect the services that its parent offers, thus if it has a malevolent parent, it will choose a low-quality route.

Divya Sharma, Ishani Mishra, *et. al.* [16] "A Detailed Classification of Routing Attacks against RPL in Internet of Things" A new paradigm known as the Internet of Things is generating a lot of scientific interest and an economic revolution because to advancements in mobile computing and wireless communications. Low power and Lossy Networks (LLN), such as wireless sensor networks and home automation systems, have been widely deployed as a result of the growing interest in this paradigm. Many embedded devices with limited power, memory, and computing capabilities form these networks, which are connected via a variety of connections such as IEEE

802.15.4 or low-power Wi-Fi. Industrial monitoring, linked homes, health care, environmental monitoring, urban sensor networks, energy management, and asset tracking are just a few of the uses for these networks.
Nasr Abosata, Saba Al-Rubaye, *et. al.*[17] "Internet Of Things For System Integrity: A Comprehensive Survey On Security, Attacks And Countermeasures For Industrial Applications" is a comprehensive survey on security, attacks, and countermeasures for industrial applications. This article primarily categorizes threats and potential security solutions in the context of IoT layer architecture. As a result, each attack is linked to one or more levels of the architecture, and a literature review of the different IoT security remedies is included.

Karen Avila, Daladier Jabba, *et. al.*[18] "Security Aspects for Rpl-Based Protocols: A Systematic Review in IoT" The Internet of Things (IoT) is a concept that has gained popularity in recent years. The wireless sensor network (WSN) has emerged as the foundation for IoT networks, and the accompanying study examines key IoT principles as well as the many security concerns that arise at the network layer. A systematic literature review is used to conduct this analysis (SLR). This type of bibliographic evaluation has become increasingly popular in recent years. Its strength is the ability to do a metric analysis, which allows you to look at both trends in the field of research you're interested in as well as relevant authors. In addition to analyzing the attacks mitigated in the RPL protocol, it is intended to identify the trend by which these attacks are reduced.

Challenges of Intrusion Detection Systems in MANETs:
Because intrusion detection systems designed for fixed networks cannot be readily implemented in the wireless network environment, research has concentrated on protecting MANETs using IDSs in recent years. In MANETs, intrusion detection is more complicated and difficult than in stationary networks.

MANETs, unlike stationary networks, lack concentration points where monitoring and data gathering may be carried out. In fixed networks, for example, traffic is monitored at network gateways, but in an infrastructure-less MANET, a node may only watch other nodes within its radio range, allowing attackers to quickly escape. As a result, ideas for network-based intrusion detection systems (NIDS) utilised in fixed networks are not immediately applicable to MANETs. Recognizing this challenge, researchers have suggested collaborative ways to audit data collecting and the use of intrusion detection algorithms based on network clustering [19, 20, 21, 22 and 23].

Classification of Network Layer Attacks
1) Passive Attacks:
Passive attacks are ones in which the attacker does not interfere with the routing protocol's functionality but instead tries to obtain useful information through traffic analysis. As a result, crucial information about the network of nodes, such as the network architecture, node location, and the identification of significant nodes, may be revealed. The following are some instances of passive attacks:

Eavesdropping
Eavesdropping is not considered a significant threat in most instances, it can offer critical information in specific scenarios, thus researchers have concentrated on reducing it. The authors of [24], for example, looked at the danger of eavesdropping as a function of the nodes' transmission range and geographical dispersion.

Traffic Analysis and Location Disclosure
As a result, traffic pattern analysis allows an attacker to identify the network's controlling nodes. Even if a message's data is encrypted, traffic analysis can still be conducted to recover some relevant information. Although passive assaults may not directly impair network operation, significant information exposure through traffic analysis or simple eavesdropping could be expensive in particular MANET application situations, such as military communication. [25, 26], and [27] are some examples of work on analysis and defense against these assaults.

2) Activated Attacks:
In active assaults, intruders perform intrusive actions such as altering, inserting, forging, fabricating, or deleting data or packets, causing different network disturbances. Some of these assaults are the result of a single intruder's action, while others are the result of a series of actions by collaborating intruders. Active attacks (as opposed to passive assaults) disrupt network operations and can be so severe that they bring the entire network down or severely degrade network performance, as in denial of service attacks. As a result, the focus of this study is on active network layer assaults. Active assaults can be further split into malicious packet-dropping attacks and routing attacks [28, 29, 30 and 31].

III. METHODOLOGY

Network backbone is important part to deliver the data from one point to other, in the recent advance of communication technology wireless is one of the most preferable medium to transfer data one location to other with low cost manner. Mobile ad hoc network form while nodes are capable to perform routing as well as distributed coordination based communication which utilizes the medium as wireless. Ad hoc network characteristics i.e. dynamic movement, low power and processing devices, decentralized coordination which excide unauthorized users to gain the resource of these types of network. In this dissertation secure the network using hybrid trust system which protect from Sybil attacks. Sybil attack is a kind of attack which captures the data from the network by identity spoofing method. Sybil attacker use the other node legitimate user ID and access the network resources that is two type same time or different time it means one class of Sybil which capture the more than one id in same time other class is in different time interval ID is change and capture the data from the network. Proposed hybrid trust calculates the trust value, in two ways direct or indirect method which protects the MANET IoT network by Sybil attack. Finally combine direct and indirect trust to calculate the final trust in this technique trust is calculate by multiple nodes who's within the range of node and resultant final trust produce by averaging to all computed trust by all nodes.

Direct Trust: Direct trust calculates by the node behavior such as ID modification, energy utilization, number of packet forwarding and number of packet dropping. Based on the ID modification it characterizes the node as Sybil attacker or no other parameter provides the information regarding the reliability of node. In mobile ad hoc network IoT based system nodes are movable that's why they are watched by its neighbors to detect the behavior of nodes.

Indirect Trust: Indirect trust means that, those parameters which indirectly produce by the attacker such are increased routing overhead, delay, minimized throughput or response etc. Sybil attacker spoofs the network by identity modification which is not authorized. Indirect trust helps to detect the misbehavior of node. Neighbour nodes watch the activity of node whose has participate in communication such activity describe in above which helps to calculate indirect trust of nodes. In the indirect trust case, some other neighbour also sends the recommendation as per based on previous history if the node previously communicate with same node that helps to strengthen the trust system to detect the Sybil attacker node.

Final Trust: The trust computation useful for detection the attack in our proposed hybrid trust module final trust computed by combination of direct and indirect trust of all neighbors and averages it. In the calculation of final trust weight are associate with respect to direct as W1 and indirect as W2 where W1=0.6 and W2=0.4 and also formalize the final trust as given in equation 1.

$$FT_i = (\textstyle\sum_{l_g=1}^{n} \quad (W1\ X\ DT_i) + (W1\ X\ IT_i))/n \qquad (1)$$

FT_i: final trust of node i
DT_i: direct trust of i node
IT_i: indirect trust of i node
l_g: l number of neighbour nodes

Trust is useful to detect the Sybil attacker node, in the proposed hybrid trust system we also analyze the node behavior during route discovery while any node frequently change the ID or use the other ID then it treated as suspicious node and trust system continues watch the particular node for further blocking to provide secure communication. After the attack detection secure routing is performing by the blocking the attacker node and source execute fresh route without the participation of attacker node.

IV. PROPOSED ALGORITHM

In this section describe how the hybrid trust method implemented in protocol development. Proposed hybrid trust module initialized by parameters i.e., number of IoT devices, routing protocol, source and destination node and execute the algorithm in step-by-step procedure. Initially source node calls the routing module and then broadcast route packet into the network, during the route searching any node use the receiver ID and send acknowledgement to source that mis-activity not recognized by source and initiate the data transmission. The proposed hybrid trust module executed by all the nodes in range whose watch the activity or every active path and calculates the direct as well as indirect trust to identify the attacker node so that block the attacker node because it's treated as Sybil attacker. Through the proposed trust system protect the IoT MANET communication by Sybil attacker and provide reliable communication.

Algorithm: Hybrid Trust against Sybil Attack in MANET IoT Network

```
Input:   $I_m$: IoT mobile devices
         $S_{j:}$ source node $\in I_m$
         $R_{l:}$ receiver node $\in I_m$
         Proto: AODV
         $n_i$: node in route
         $FT_i$: final trust of node i
         $DT_i$: direct trust of i node
         $IT_i$: indirect trust of i node
         $l_g$: l number of neighbour nodes
         $W_1$: 0.6 weight
         $W_2$ = 0.4 weight
         $\Psi$: Radio Range
Output:  Detection Accuracy, Energy Consumption, Number of Packet Receives, Throughput [bps], Routing Overhead
Procedure:
Step1:   $S_j$ call routing proto(AODV)
Step2:   $S_j$ broadcast (AODV, $S_j$, $R_l$)
         While (nodes in $\Psi$ & node != $R_l$)
                 Node update id as $R_l$
                 Send acknowledge to $S_j$
                 $S_j$ start sending data
         End while
Step3:   Hybrid Trust execute by (neighbors)
         Neighbors $l_g$ watch $n_k$ node which participate in route
                 $l_g$ calculate $DT_n$ & $IT_n$ of node $n_i$
                 Compute $FT_i = (\sum_{l_g=1}^{n} \quad (W1\ X\ DT_i) + (W1\ X\ IT_i))/n$
                 If $FT_i$ < 0.6 & $l_g$ detect id modify Then
                         Block $n_i$ node
                         $S_j$ call routing module
                         $n_i$ not in route while execute fresh route
                 Else
                         $n_i$ is not attacker
                         Permit to belongs in route
                         $n_i$ send data to receiver node
                 End if
```

V. PROPOSED ARCHITECTURE

In proposed hybrid trust architecture shown in figure 1 which is represent IoT based MANET device who want to sends the data to receiver than it calls the routing module. In MANET routing ad hoc on demand distance vector (AODV) is most suitable for shortest path that's why use the routing protocol as AODV which broadcast in network.

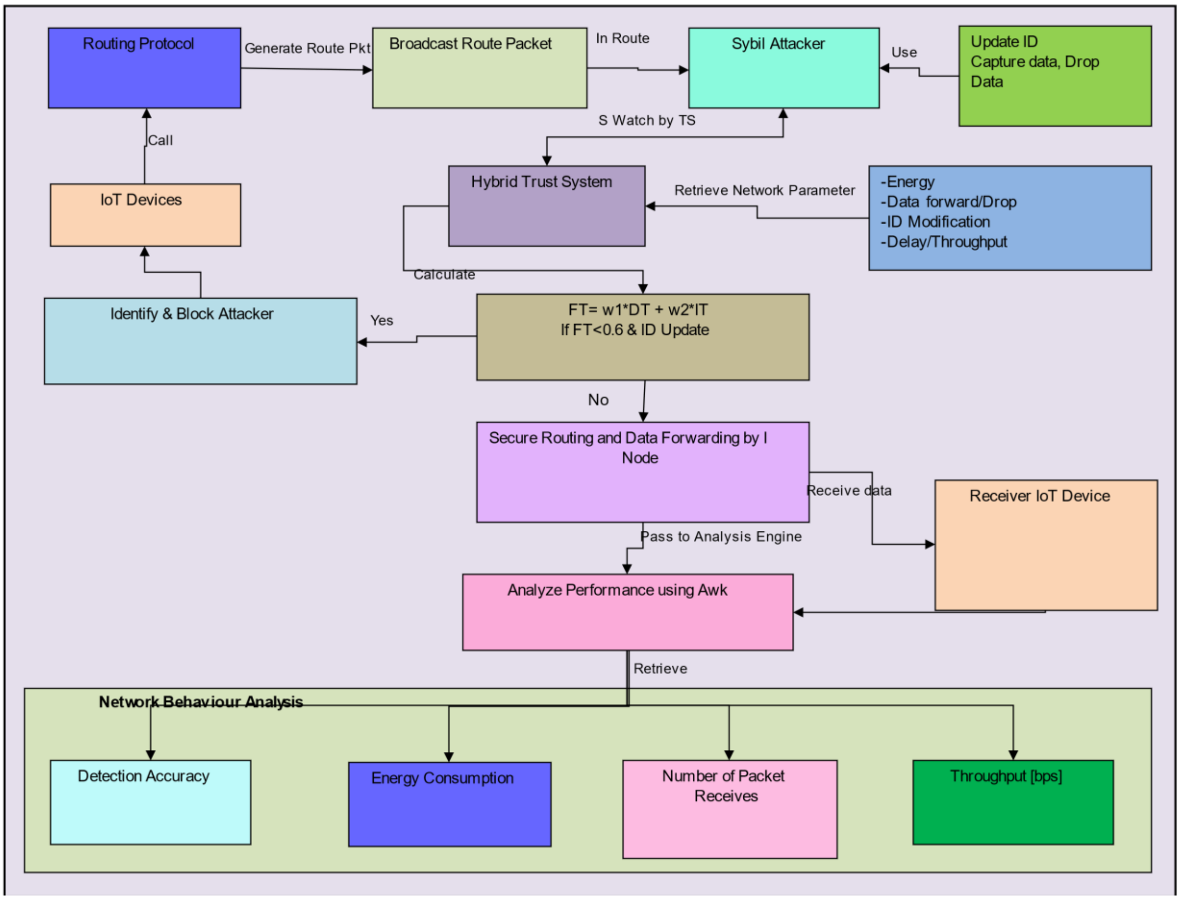

Figure 1: Basic Interface Architecture of NS-2

While the broadcasted packet comes in to Sybil attacker who use the updated ID which is equal to destination ID than it immediately sends the reply packet to source node. In the data transmission phase source node instantly start data sending module without knowing the detail about attacker and data receives by Sybil attacker and drop or misuse those arrived data. But proposed hybrid trust system watches every activity of its neighbour during route discovery as well as data transmission phase and calculates direct and indirect trust of its active device in path. Finally total trust is evaluate based on the node behavior, while final trust found less than 0.6 and updated ID it means node as Sybil attacker and block that node by proposed security system else treated as genuine node and evaluate the outcome of proposed security in terms of throughput, energy consumption, number of packet receives and packet drop etc.

VI. RESULT DISCUSSION

A. Simulation Parameter

The simulations parameters are considered for simulation of both the modules are mentioned in table 1. The simulation is providing the almost result accuracy if the network will implement in real time. The security scheme is really effective for securing network from Sybil attack. The parameters are also play an import role in routing, energy consumption and other performances also. The simulation is not performing in single node density scenario but measures in different node density scenarios in MANET IoT network.

Table 1 Simulation Parameter

Network	MANET
Simulation Environment	1000*1000
Types of Antenna	Omni-Direction
Propagation Type	Two Way Ground
No. of IoT Devices	30, 40, 50, 60
Energy Model	Initial 100 Joule
Network Protocol	AODV
Transport Layer	TCP, UDP
Security Technique	SecTrust, Hybrid Security
Application Data	CBR
Message length	1024bit
Mobility	Random
Random Waypoint	Node speed= Random
Simulation Time	50 Seconds

Detection Accuracy Analysis

Detection Accuracy is an essential performance statistic used to assess the effectiveness of a security mechanism in a network. In terms of PDR, this graph depicts the performance of both systems. The suggested method outperforms the prior scheme in terms of performance, and this is due to the fact that it not only secures the network but also performs efficient routing. Due to packet loss in the network, the performance of traditional energy-based routing is not computed all the way to the end of the simulation. In this figure the proposed Sec trust system has a percentage of receiving around 99 percent, whereas the existing hybrid trust plan has a detection accuracy is approximately 94 percent. This indicates that the network's performance has increased by roughly 5% as compared to the prior design

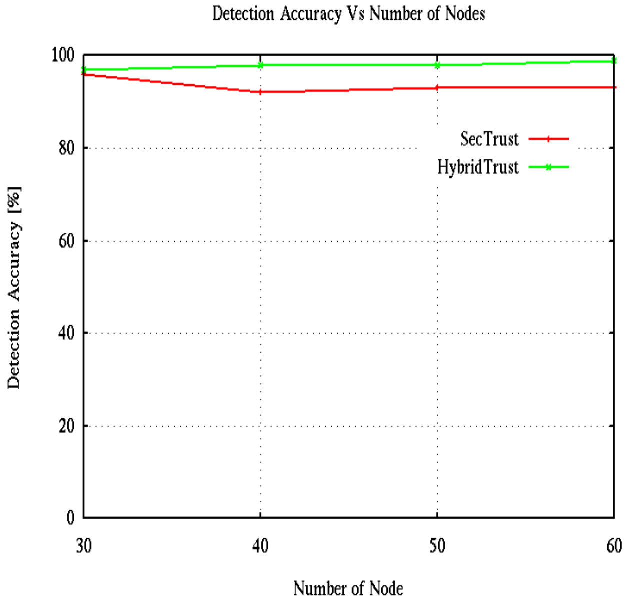

Figure 2: Attack Detection Accuracy

B. Energy Consumption Analysis

The life of mobile nodes in MANET IoT is totally battery dependent, and these nodes will not function correctly unless they have enough battery power. To increase network lifespan, energy-efficient sensor node communication is required. The Sybil attacker reduces network performance, but both methods are capable of securing networks and providing dependable routing performance. Total energy consumption is an essential component in determining the performance of an energy-based procedure. Because we are starting the communication from full battery power, the beginning energy of the nodes is not need to be the same. When compared to the Sec trust method, Hybrid Trust consumes more energy. Hybrid trust performs better in all node density scenarios, and the rationale is simply to select the most reliable and secure way for routing with IoT devices.

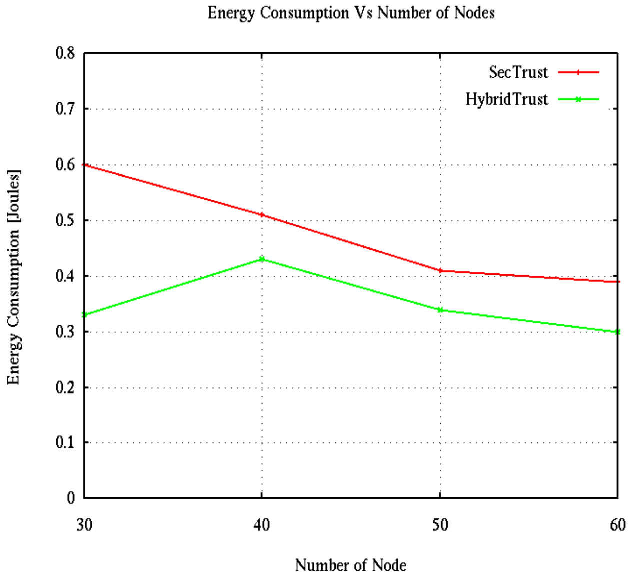

Figure 3: Energy Consumption Analysis

C. Number of Packet Receives Analysis

The effective receipt of data is simply one approach to improve the routing performance of an IoT network. The connection behavior is of both sorts, in that acknowledgement (ACK) is received after successfully receiving data in connection fewer protocols and no ACK is received in connection more protocols. ACK is critical in terms of security. In this graph, the number of data packets received in the case of hybrid Trust is greater in all node density situations. Now, in the case of Sec trust, around 4000 packets are received in the network, but in the case of Hybrid Trust, approximately 500 packets are received in the network in 60 node density. The attacker decreases network speed, whereas the security strategy improves it by removing the attacker infection. In this case, Sec trust is adequate for network security, but hybrid Trust provides security and an effective routing method in an IoT network.

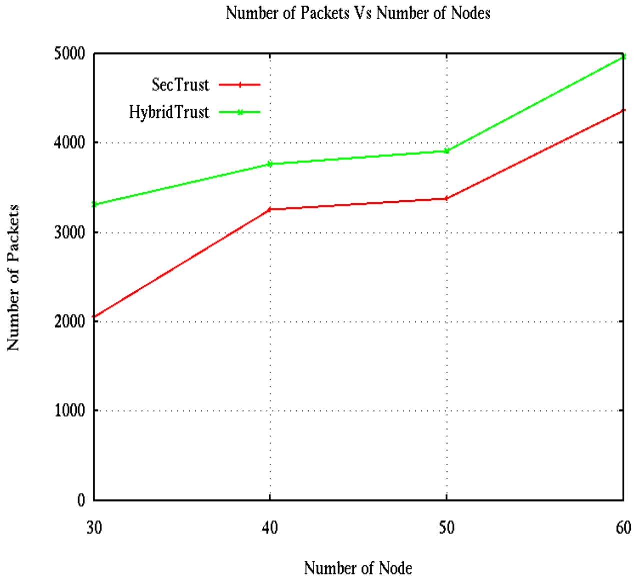

Figure 4: Packet Receive Analysis

D. Throughput [bps] Analysis

Throughput analysis measures network performance in bits per second (bps). In a MANET IoT network, throughput is measured by counting the number of packets received per unit of time. This graph depicts the throughput in the proposed Hybrid Trust system and the existing Sec trust method in the face of a Sybil attack. In this situation, the proposed methods outperform the prior security system in terms of throughput performance. In the event of Hybrid trust, the nodes in the network use their energy for communication rather than wasting it on retransmission. In all node density scenarios, high throughput is important. In the Hybrid Trust scheme's 60 node density scenario, the high throughput value is around 130bps. It indicates that the network's life and the number of packets sent in the network are longer than in the prior system.

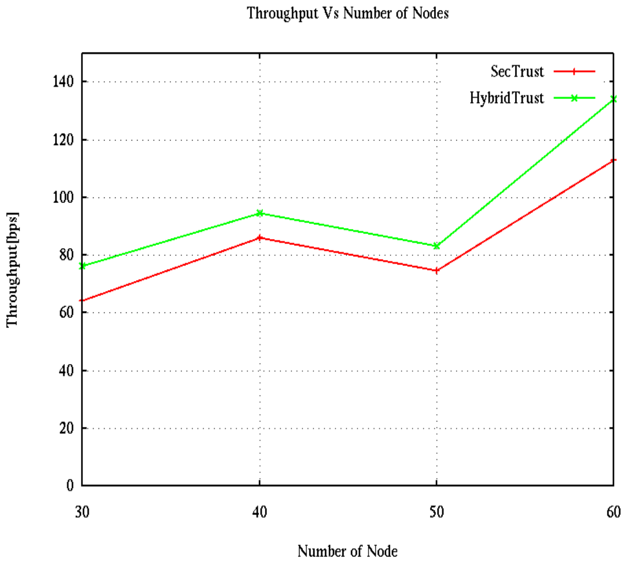

Figure 5: Network Throughput [bps] Analysis

E. Routing Overhead Analysis

Routing packets are transmitted in the network to establish a link between the sender and the destination. Following the transmission of routing packets, data packets are sent between the sender and the recipient. The routing overhead is calculated in relation to the total number of data packets successfully received at the destination. This graph depicts the routing overhead performance of the Sec trust and Hybrid Trust schemes in a MANET IoT network against a Sybil attack. In this scenario, Sec trust has a maximum routing overhead of around 2.5 up to the end of the simulation duration, whereas Hybrid trust has a maximum routing overhead of about 2.1 in the network. The suggested technique results in better packet reception since the overhead is kept to a minimum. It implies that Hybrid Trust performs better with fewer routing packets, and it also benefits from energy savings from overhead packets flooding in the network.

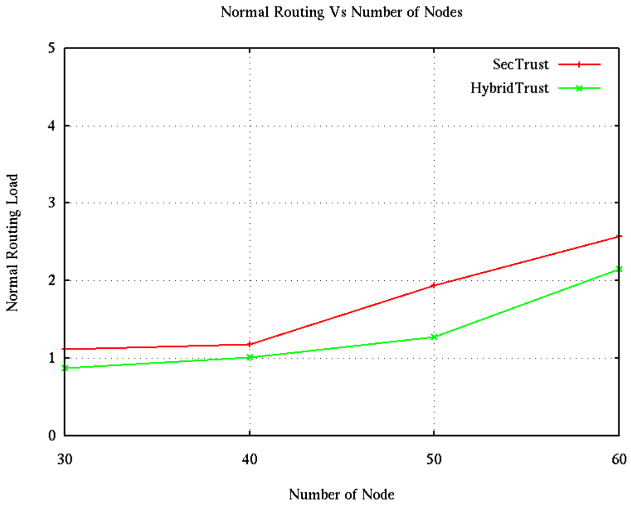

Figure 6: Routing Overhead Analysis Vs Number of IoT Nodes

VII. Conclusion and Future Scope

The Sybil attacker is not like other attackers that have a single identity, and it is very difficult to create a new Hybrid Trust technique that is better than the existing Sec Trust approach for identifying them. Because MANET nodes' capabilities are intrinsically limited, providing safe routing in IoT is a hard and difficult undertaking. For assaults, a number of countermeasures have been offered in the literature. We concentrated on the rank and Sybil attack in particular. Although a variety of remedies have been offered for this attack, the majority of them contain weaknesses that render them useless for large-scale IoT installations. The identification of Sybil attackers is not easy, but Sec Trust can achieve it while simultaneously returning the performance to normal. The proposed Hybrid trust architecture not only provides safe routing but also makes optimal use of network resources such as electricity and node battery capacity. Communication between IoT nodes is difficult in the presence of the Sybil attacker. The hybrid trust scheme consumes 0.1 joule less energy in 60 node density and the throughput is about 50bps more. The detection accuracy of hybrid trust scheme is showing 5% improvement in performance. The packet reception is improved, and network overhead is decreased owing to less flooding of other packets (not including data). The efficient utilization of bandwidth increases the data rate, which improves throughput. The remainder of the measurements indicates improved performance in all node density scenarios. Sec Trust also delivers trusted performance, but Hybrid Trust enhances both trust and routing performance in IoT networks.

As we know that the Sybil attacker changes its identity, and the node identification is difficult in a dynamic network. The security strategy computes the trust value, and this trust value determines whether or not the communication is free of attackers. The existence of many attackers may also be identified in a network by calculating the trust value. Because Sybil and Vampire attackers have very distinct behaviors, the suggested Hybrid Trust Scheme to protect routing in IoT will need to be changed in the future.

REFERENCES

[1] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," Ad Hoc Networks, **vol. 1, no. 1, pp. 12-64, 2003.**

[2] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," RFC 4838, **IETF**, **2007.**

[3] J. N. Al-Karaki, and A. E. Kamal, "Routing Rechniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communications, **vol. 11, no. 6, pp. 6-28, Dec. 2004.**

[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A urvey," Computer Networks, **vol. 54, no. 15, pp. 2787-2805, Oct. 2010.**

[5] P. Juang, H. Oki, and Y. Wang, "Energy Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet, "International Conference on Architectural Support for Programming Languages and Operating Systems, San Jose, CA, Oct. 2002, pp. **96-107**.

[6] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," IEEE Wireless Communications, **vol. 14, no. 5, pp. 85-91, Oct. 2007.**

[7] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, "On the Efficacy of Frequency Hopping in Coping with Jamming Attacks in 802.11 Networks," IEEE Transactions on Wireless Communications, **vol. 9, no. 10, pp. 3258- 3271, October 2010.**

[8] Aditya Tandon, Prakash Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT" 2019 **IEEE**.

[9] Ismail Butun, Member, IEEE, et.al."Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures" Manuscript received March 5, **2019**.

[10]Wang, Yizhong, **"**Secure routing protocol over mobile Internet of Things wireless sensor networks" Monterey, California **2018**.

[11]Ruchi Mehta, M.M.Parmar, "A Survey on Security Attacks and Countermeasures in RPL for Internet of Things"IJARSE April **2018**.

[12]VISHAL SHARMA, (Member, IEEE), et. al "Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey" IEEE ACCESS Received July 28, 2020, accepted August 26, **2020**.

[13]Hassan I. Ahmed, Abdurrahman A, et. al."A survey of IoT security threats and defenses" International Journal of Advanced Computer Research, **Vol. 9(45), 2019.**

[14]Weidong Fang, Wuxiong Zhang,et.al**.**"Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey" Hindawi Wireless Communications and Mobile Computing Volume **2020**,

[15]Anhtuan Le, Jonathan Loo, Aboubaker Lasebae et. al."The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks" IEEE Sensors Journal, **Vol. 13, No. 10, October 2013.**

[16]Divya Sharma, Ishani Mishra, et. al. "A Detailed Classification of Routing Attacks against RPL in Internet of Things" **2017**, **IJARIIT**.

[17]Nasr Abosata, Saba Al-Rubaye Et.Al. "Internet Of Things For System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications" Sensors **2021**.

[18]Karen Avila, Daladier Jabba, et. al. "Security Aspects for Rpl-Based Protocols: A Systematic Review in IoT"MDPI Published: 17 September **2020**.

[19]D.Sterne, P.Balasubramanyam, D.Carman, B.Wilson, R. Talpade, C.Ko, R. Balupari, C.-Y. Tseng, T.Bowen, K.Levitt and J.Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs", Proc. IEEE International Workshop on Information Assurance (IWIA 05), **2005**.

[20]Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks, New York, USA, **2003**.

[21]B. Pahlevanzadeh and A. Samsudin, "Distributed Hierarchical IDS for MANET over AODV", Proc. IEEE International Conference on Telecommunications, Malaysia, May **2007**.

[22]Soni G., Chandravanshi K., Jhariya M.K., Rajput A. (2022) An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET. In: Sarma H.K.D., Balas V.E., Bhuyan B., Dutta N. (eds) Contemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems, vol 281. Springer, Singapore. https://doi.org/**10.1007/978-981-16-4244-9_5**

[23]P. Yi, Y. Jiang, Y. Zhong and S. Zhang, "Distributed Intrusion Detection for Mobile Ad Hoc Networks", Proc. IEEE Application and Internet Workshop, **2005**.

[24]G. Soni, M. K. Jhariya, K. Chandravanshi and D. Tomar, "A Multipath Location based Hybrid DMR Protocol in MANET," 2020 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE), pp. **191-196**, **2020.** doi: 10.1109/ICETCE48199.2020.9091778.

[25]J.C. Kao and R. Marculescu, "Eavesdropping Minimization via Transmission Power Control in Ad Hoc Wireless Networks", Proc. IEEE Sensors and Ad hoc Communication and Networks SECON, **2006**.

[26]T. He, H. Wang and K.W. Lee, "Traffic analysis in anonyms MANETs", Proc. IEEE Military Communication Conference MILCOM, November **2008**.

[27]J. Kong, X. Hong and M. Gerla, "A new set of passive routing attacks in Mobile ad hoc networks", Proc. IEEE Military Communication Conference MILCOM, October **2003**.

[28]E. Perkins and M. Royer, "Ad Hoc On Demand Distance Vector Routing", Sun MicroSystem Laboratories Advance Development Group, Proceeding of the IEEE MOBICOM, pp **90-100**, 1999.

[29]B. Johnson and A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Proc. Mobile Computing Journal, **Vol.353, pp 153-181, 1996.**

[30]Kamlesh Chandravanshi, Akrosh Tiwari And Mukesh Bathre, "Intrusion Detection system in Wireless Ad-Hoc Network", Computer and Network Technology, pp. **267-271**, **2009.** https://doi.org/10.1142/9789814289771_0052

[31] M. Pirrete and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defence", International Journal of Distributed Sensor Networks, Vol.2, No.3, pp **267-287**, **2006.**

AUTHORS PROFILE

Mr. PRINCE KUMAR completed Bachelor of engineering (B.E) from J. N. College of Technology, Bhopal, India in year 2017. I am currently pursuing my Masters of Technology (MTECH) from Technocrats Institute of Technology (TIT) , Bhopal , India since 2018 . My area of research is mobile adhoc network and security.

Dr. Rachana Kamble an Associate professor, Department of Computer Science & Engineering, Technocrats Institute of Technology, Bhopal M.P. She has been involved as a member of research degree committee and member of board of studies for various Institutes & Universities. With over two decades of teaching and Software Development experience, she has been guiding the students for their master studies, Projects and Research Work. She has over a decade of teaching experience in some of the reputed engineering institutions. She has been author and Co-Author of many books in field of Computer Science, Information Technology, Computer Security, Cryptography and Network Security, Ethics of Cyber Security, Data Science, Cloud Computing: principles and paradigms, Internet of Things Challenges, Advances and Applications and many more. "JAVA CAMPUS CRACKER (IN 21 DAYS)" -This academic textbook refers for Kindle edition.