RTBSAD: RSSI AND TRUST-BASED SYBIL ATTACK DETECTION IN MANET

Meena Bharti

Research Scholar, Department of Computer Science and Engineering,
I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India.
meenabharti89@gmail.com

Shaveta Rani

Professor, Department of Computer Science and Engineering,
Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, 151001, INDIA
garg_shavy@mrsptu.ac.in

Paramjeet Singh

Professor, Department of Computer Science and Engineering
Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, 151001, INDIA
param2009@mrsptu.ac.in

Abstract

The limited and resource-constrained nodes in Mobile Ad hoc Network (MANET) make it vulnerable to attacks. A Sybil node poses a serious threat to the security of the network as a Sybil node pretends to be another node and manipulates the network. The already existing solutions are by using encryption keys RSSI-based and trust value-based Sybil attack detection. The encryption key method is expensive while RSSI- based solutions have high false-positive and trust value-based solutions are slow in the detection of Sybil node. In this study, a new way is proposed to detect Sybil attacks using a combination of RSSI and Trust values to take leverage of both schemes while overcoming their disadvantages. The proposed scheme RTBSAD is compared with existing schemes in terms of True detection Rate, Average Energy Consumption, etc. The results showed that the proposed scheme outperformed the existing schemes.

***Keywords*: MANETs; Sybil attacks; Received signal strength indication; Trust value.**

1. Introduction

MANETs present unique security challenges that can also provide opportunities. Different types of Network Security include Availability, Integrity, Confidentiality, and Authentication [Wu et al., (2006)]. There are many different ways to try and exploit the vulnerabilities in MANET. These are a connected network of mobile devices that don't need to be near each other and don't need to be connected to any central Wi-Fi. In this setup, each mobile device acts as a router when the source and destination of a packet are within range. The messages can be transmitted back and forth between the sender and the receiver when they are within the range [Zhong et al., (2004)]. MANETs are most useful in emergencies or military crises when there is no pre-existing infrastructure. Network security in MANETs is difficult to maintain due to its dynamic topology and limited resources. Lack of centralized identity management makes them more vulnerable to attacks [Bhise et al., (2016)]. Many attacks like DoS, jamming, Sybil, black hole, and gray hole [Douceur, (2002); Shah et al., (2021)] happen in these networks. Sybil attacks happen when multiple identities are created by the person who is responsible Wireless networks use unique identifiers that identify the person. These addresses are used for communication with the network entity It is easy to get the identity of a node altered or stolen by an adversary [Douceur, (2002)]. The slight problem arises from the fact that two nodes cannot have the same identity when they are separate. This can create a really big problem if one node is using the identity of several other nodes to steal their content [Douceur, (2002)].

Sybil attackers have several ways to disrupt ad-hoc networks [Newsome et al., (2004)] such as: For example, a Sybil attack benefits the attacker by disrupting multipath routing, which makes it appear as if they are new nodes within the network. To maximize their disruptive nature, they can also mimic existing nodes or create new ones. Hyperlocal reputation and trust schemes could be disrupted by Sybil nodes as malicious nodes are capable to escalate their trust. They can also do this by exploiting their virtual identities. With wireless sensor networks, for example, attackers might create fake data readings. For example, Sybil attackers could spoof lots of different nodes to change the aggregate reading result [Hill et al., (2002)]. It is easy to create a new node with this system because there are no restrictions on the number of nodes each individual can create. Sybil attackers can manipulate voting-based systems by controlling multiple identities.

The Sybil attacks are dangerous for the normal operation of the network and to secure MANET. As such, they need to be responded to and eliminated as soon as possible. Sybil attacks must be addressed immediately and eradicated as soon as possible. Algorithms consume a lot. They can drain batteries quickly if they rely heavily on communication. Solutions [Golle et al., (2004)] that use a key exchange to vouch for authentication and identity can drain a lot of power because they require the distribution and piggybacking of random keys in messages. Every node has its resources and you must monitor your memory usage.

In recent studies [Abbas et al., (2009); Demirbas et al., (2006); Paul et al., (2017); Wang et al., (2007); Yao et al., (2017), (2018)] RSSI-based solution is provided, which is preferable because it doesn't require sharing the key with the MANET and can prevent the adversary from Piggybacking messages. When you message someone and they reply, it's only fair to mention your signal strength. Otherwise, if the sender ID is different but the RSSI are similar, you'll get an instant message from them asking what's going on because it doesn't make sense. One downside of this scheme is that RSSI [Newport et al., (2007)] varies inconsistently, making it unreliable[Zhou et al., (2004)]. Additionally, since Sybil nodes can control their transmission power and ID number in MANETs [Gay et al., (2003)], the original ID can be easily changed by sending out a false location. RSSI is dependent on power, so if a transmitter sets its power to destroy the signal, then the RSSI will be 0.

Trust management also make assure to the protection of safety for nodes that are connected [Alsaedi et al., (2017); Bali et al., (2016); Boukerch et al., (2007); Chakeres et al., (2004); D'Angelo et al., (2019); Kim et al., (2015); Liang et al., (2019); Priyadarshi et al., (2019); Sun et al., (2019); Xie et al., (2013); Zheng et al., (2014)]. In a recent study, a technique is provided to detect Sybil attacks in MANETs by a combination of RSSI measurements and trust values. It is lightweight, resistant, and detects Sybil attacks with high accuracy. Our solution is light because it only needs one other node alongside the receiver.

Although experiments have shown that the RSSI is unreliable and changes over time, by measuring it from several receivers at once, we can account for these variations [Zhou et al., (2004)]. RSSI ratios were first proposed by [Zhong et al., (2004)] but the success of this approach has only been shown now. We've seen a lot of variability in RSSI values when there is only 1 receiver. The best way to get a stable connection is to use multiple receivers and calculate their ratio. By doing this, we found the range varied less than one mile.

A lightweight solution is possible by not calculating the position of the sender. We do this by not calculating fading distances and also relaxing the computation requirements. Furthermore, we show through experiments that two nodes are enough to detect Sybil nodes in a 3-D coordinate system, which is way fewer than the four-receiver nodes required in theory [Zhong et al., (2004)]. We provide a practical solution for the multipath model.

The following sections cover some of the key points in this paper. Section 2 is about the literature review, while Section 3 is an overview of our proposed approach. In Section 4 we will share our findings. This paper concludes in Section 5.

2. Literature Review

The growth of the internet is expanding exponentially. With this growth, mobility in sensor devices is an upcoming trend. We use a mobile device with internet connections, which becomes connected. So, the security of data passing through these devices is a major concern. Many researchers so far have worked in this field. The work done by various researchers in this field is listed in this section.

[Capkun et al., (2005)] show the use of mobility to make MANET more secure. Solutions that use a lot more energy are typically more costly and will cost even more over time. The authors recommend something else with which one can communicate securely and anonymously over the internet. They contacted correspondents by wired or infrared media to authenticate their identity and obtain a point-to-point encryption key. By encrypting a user's identity using a blockchain, the authors hoped to prevent impersonation as well as Sybil attacks. A5 devices assume that many of these nodes are wirelessly connected or infrared.

Mobile networks have security issues that can be very worrying. [Bettstetter et al., (2003)] propose that this type of network does not require fixed infrastructure. Sybil attacks happen when someone with internet access uses multiple social network accounts to influence the opinions of others. These kinds of attacks pose a danger to decentralized systems. A passive ad hoc identification systems and key distribution are two ways to protect yourself from this kind of attack. An adversary can't be alerted to our presence by using a detection network. An attack would have multiple detection nodes fooled to work. This is why network decentralizations such as peer-to peer networks or geographical routing protocols depend on this method.

[Zhou et al., (2004)] The DCA uses a cryptography type that is protected from MANET security threats in this method. Sybil attacks can occur when someone attempts to create multiple identities. Symmetrical key authentication processes are used. This is where threshold cryptography employs the concept of distributing a signing process to n Nodes. Intruders will have difficulty obtaining 'k' for the signing process and gaining certification. This method has only two keys, which can be compromised by someone to gain access. A distributed certification authority was created to address this problem.

[Abbas et al., (2009)] suggested that the Sybil node be identified using a one-time identifier. The RIL decides whether a node is allowed to be forwarded. Otherwise, packets could be lost. A new node that arrives in your network will be checked to see if it can be forwarded. If the neighbor accepts it, the node will be added to the Registered Identity List. The node can be removed from the RIL once a Sybil identity is received from its neighbor. To overcome the problem of Sybil identities sending fake reports about nodes to blockchain nodes must wait for this report to be received from one of its neighbors. If a node doesn't get a signal from other nodes within the allotted time, it will not be able to establish its location and can't connect.

[Piro et al., (2006)], in their method, PASID, is the technique they use to monitor all of your identities over time to tell you how many nodes you have at any given point. The length of time the data is sent varies based on how mobile the nodes are. If it's being sent wirelessly, each node has its frequency to transmit from. Legitimate nodes will be active and roam around the network, transmitting via their channels. If your network is Sybil, all the data will still move along in series (i.e.) sends in a pipelined manner. In other words, if an attacker controls many nodes, no matter the data's origin or owner, the attackers' channel will be used too.

[Abbas et al., (2012)], in this way, Sybil's behavior and legitimacy are determined by the entry/exit points of the nodes they are connected to. This divides the node's radio spectrum into two zones: the White and Grey zones. Legitimate nodes begin in the "grey area" and then increase their activity with time. Fake Sybil Nodes or Sybil nodes mimic the behavior of legitimate nodes to gain credibility. RSSI values remain stable even if the node has changed its identity. This means that the RSSI value has changed. When one is in an interference pattern, the transmission rate can have an impact on the signal strength they receive from their device. Signal strength is a measure of speed, and fast-moving nodes are often detected first. This can lead to higher false-negative rates.

[Zhong et al., (2004)], in this method, nodes cannot have their position hidden from four or more nodes. Monitors can be identified by their signal strength and SNR. You can select monitors from a list of nodes that are near each other and place them side-by-side. The node position is determined using data from the received signal, including power and speed, radiofrequency, and traffic intensity. This method can help you find interfering nodes if they occur. However, static nodes need to be pre-defined and monitored by 4 nodes that stay static during the process. Scenarios not discussed yet.

A lot of research has been done in the field of Sybil attack detections. Various authors used different kinds of techniques. Some authors used cryptography, RSSI-based solution, and trust management-based solution. Although cryptography is an effective solution to prevent attacks it is costly. On the other hand, RSSI and trust management-based solution is less costly but there is a chance of high false-positive in the case of RSSI-based solutions while trust management detection is slow in the detection of Sybil attacks. So, in the present paper, we tried to address this gap by combining RSSI and trust management in such a way that we can overcome the disadvantage of both solutions and find an optimal way to detect Sybil attacks.

3. Proposed Work

Sybil nodes join the network multiple times with fake identities. This can affect many operations of a network like routing, voting, data aggregation, etc. Sybil attack can be of two types one in which Sybil identity is created and then after some time its history is deleted. This kind of attack is called a whitewashing attack while in the second form several identities are created simultaneously. The work done by previous authors is either based on RSSI values or trust-based models. RSSI-based Sybil attacks detection [Abbas et al., (2012)] identifies new nodes that enter the radio spectrum of another node. Although this scenario detects the Sybil node at the initial phase there are high false positives in this method. As in the case of RSSI value, the need for nodes is noted based on the first RSSI value encountered which will encounter when the node will send some message. If that first encounter of penetration of node is higher than the threshold value then the node is detected as a Sybil attack. But sometimes a legitimate node says node A is entering into the radio range of node B. But while entering it has lost connection or due to traffic not being able to send or receive a message, so when node A will be observed by node B it might have penetrated B's radio range higher than the threshold value so this node will be detected as false positive. Apart from this sometimes the Sybil node's radio range can be detected at a lower threshold value so can be left undetected. On the other hand, trust-based Sybil attack detection is a more prominent technique but to make trust node has to make a history of forwarding messaging which is a time-consuming process thus node will be detected in later stages till then we can have a loss of packets. To overcome this issue, we have combined both techniques to take the advantage of both techniques.

3.1. Assumption of network

The structure of the network is shown in Fig. 1. There is a base station that also acts as a sink. The node can communicate omnidirectional. All nodes are homogenous having the same initial energy and same radio range. The network is divided into clusters. Firstly, nodes are chosen as cluster heads based on their residual energy and link quality with the base station. Initially, the base station will initialize the energy of sensor nodes, each node will add itself to the cluster according to its distance from the cluster head. Each sensor node can send messages to the cluster head directly or through another sensor node. Nodes having residual energy of less than 20% will perform basic activities only. Each node will maintain two arrays, one this trusts value with neighboring node. Others will list the Sybil node. Only a legitimate node can act as a cluster head. As we have combined RSSI value and a trust-based model to reduce false positives. We have kept the RSSI penetration threshold bit high. The nodes which are still left undetected in the RSSI layer will be detected in the trust model.

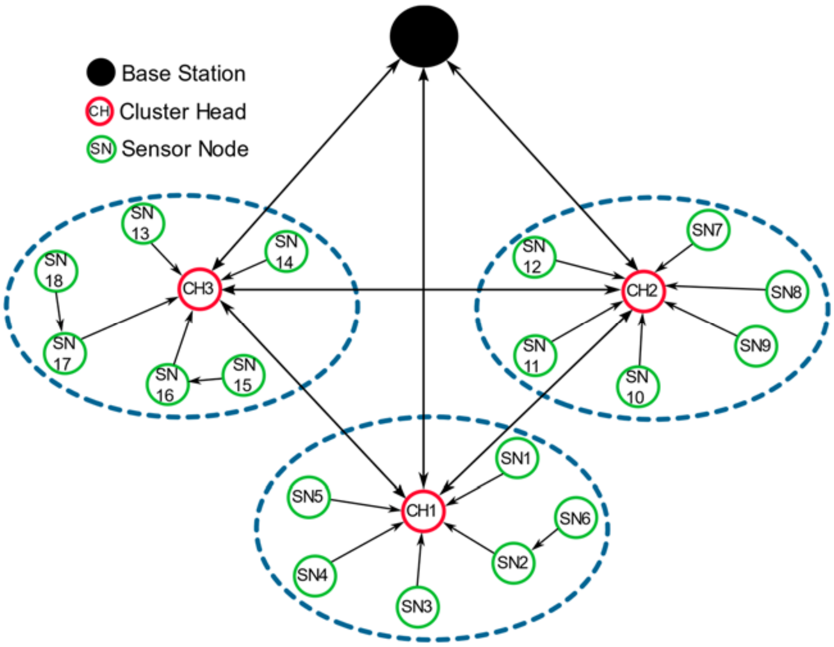

Fig. 1. Clustered network

3.2. Detection Model

Two-layer models are proposed to detect Sybil attacks. The first layer RSSI value is recorded for the incoming node. Consider a node named A. Its radio spectrum is divided into two zones: green and red. The assumption is that legitimate nodes will only enter radio ranges of node A slowly. Sybil node is likely to appear suddenly in your neighborhood. This will allow the Sybil node to penetrate more into the radio range radio spectrum of A than a legitimate one. Based on this, a node that, makes its first observation in the green zone is considered legitimate and the node that is seen in the red zone is considered to have a Sybil node. The scenario of node A, node B and node C is shown in Figure 2. Node B and Node C are entering into the radio range of node A. Node B is firstly observed in the green zone and hence is considered a legitimate node while node C makes its first observation in the red zone and hence is considered a Sybil node.

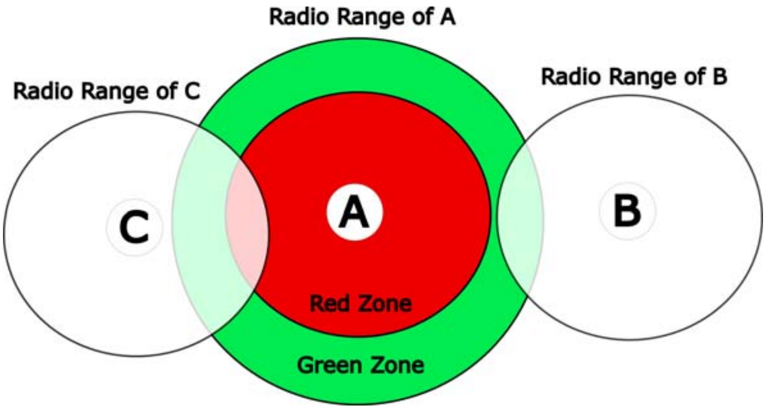

Fig. 2. Zone distribution of nodes

There can be false positives in Sybil node detection using RSSI value as sometimes a legitimate node enters in the radio range of say node A but due to traffic or loss of connection, it may be the case that, the node is not observed by A in the green zone. So, this node will penetrate deeper into the radio range of A and will be firstly observed in the red zone and hence will be declared as Sybil. To avoid such situations, we have increased the area of the green zone as compared to this area in lightweight Sybil attack detection [Abbas et al., (2012)]. The Sybil nodes left undetected will be detected in the second layer consisting of the trust model. For the trust model, direct and indirect trust values are used. Direct trust is calculated based on a number of correct packets delivered by a node for which the trust value is calculated. To calculate direct trust, consider node X is calculating the trust value for node Y, then direct trust can be calculated using Eq. (1).

$$DT_{XY} = \frac{Correct_{packets_{forwarded_{XY}}}}{Total_{packet_{recieved_{XY}}}} \quad (1)$$

Sybil node when join multiple times tries to increase the trust values of its fake node and decrease the trust value of another node. To prevent the network from this bad-mouthing due to the Sybil node, an indirect trust value is used. To calculate indirect trust from node X to Y Eq. (2) is used.

$$IDT_{XY} = \frac{\sum_{i=0}^{N} DT_{Neighbour_{i,Y}}}{N} \quad (2)$$

i.e. Neighbors of Node *X*. *N* is a total number of neighbors of *X*. The final trust value is calculated using Eq. (3)

$$D_{XY} = w_1 \times DT_{XY} + w_2 \times IDT_{XY} \quad (3)$$

Where $w_1 + w_2 = 1$, The values of weights can adjust according to application and deteriorate the effect of Sybil attack. The steps of the algorithm are as follows:

Algorithm 1: Sybil nodes detection

Input: Sensor nodes, their location, and initial energy

Output: Detection of Sybil nodes

```
(1) Initialize sensor nodes with coordinates, energy and trust values
(2) Communication of nodes start
(3) If $node_{energy}$ < 20% of initial energy
        i. Then this node will not take part in communication
(4) Calculate RSS value at entry
(5) If RSS > $threshold_{RSS}$ value
(6) Put it in a malicious list and broadcast
(7) Calculate direct trust for say node X to Y using Eq. (1)
        $DT_{XY} = \frac{Correct_{packets_{forward_{XY}}}}{Total_{packets_{recieved_{XY}}}}$
(8) Calculate indirect trust for node X to Y using Eq. (2)
        $IDT_{XY} = \frac{\sum_{i=0}^{N} DT_{Neighbour_{i,Y}}}{N}$
(9) Find the final trust value using eq (3)
        $D_{XY} = w_1 \times DT_{XY} + w_2 \times IDT_{XY}$
(10) If $D_{XY}$ > $threshold_{trust}$
     Put node in malicious node and broadcast
(11) CH will send a message to the Base station regarding the Sybil node.
(12) Base station will remove this node.
```

4. Simulation and Results

The simulation of the proposed work RTBSAD is done using MATLAB R2018a. The comparison of the proposed work is done by Almas et al. [Almas Shehni et al., (2018)], Rafeh et al. [Rafeh et al., (2014)] and Jamshidi et al. [Jamshidi et al., (2018)] in terms of True Detection Rate (TDR), False Detection Rate (FDR), Average Energy Consumption and Packet Delivery Ratio (PDR).

4.1. TDR

TDR is True Detection Rate. It calculates using Eq (4)

$$TPR = TP / (TP+FN) \quad (4)$$

Where TP is True Positive and FN is False Negative. Higher the true positive rate better is than the detection policy. The comparison of the proposed work with Almas et al., Rafeh et al., and Jamshidi et al. in terms of TDR (in percentage) is shown in Table 1 and Fig. 3.

Sybil nodes in network (in Percentage)	Almas et al.	Rafeh et al.	Jamshidi et al.	RTBSAD
10	80	75	73	82
20	70	68	70	71
30	64	60	62	64
40	60	55	58	62
50	53	52	54	60
60	50	46	51	55

Table 1: Comparison of RTBSAD with existing techniques in terms of TDR (in percentage)

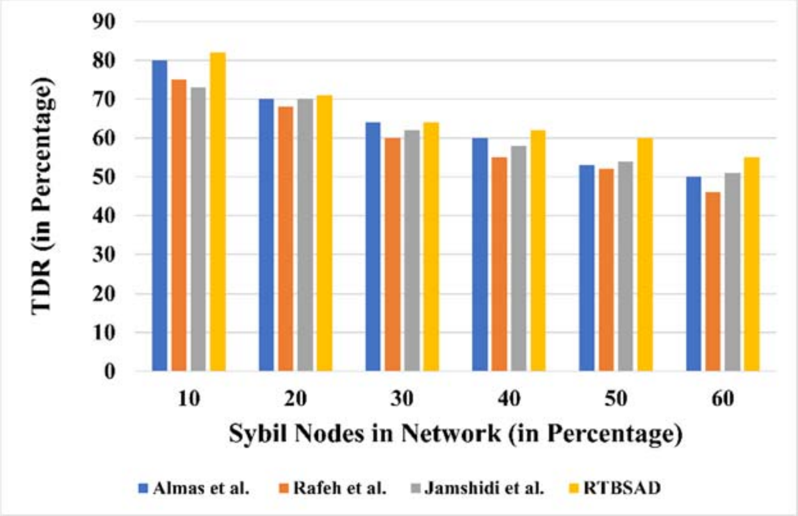

Fig. 3. Graphical representation of TDR result of the proposed scheme with existing schemes

The TDR of RTBSAD is 9% higher than Almas et al., 19.5% higher than Rafeh et al. and 7.2% higher than Jamshidi et al. when 60% of Sybil nodes are added into the network.

4.2. FDR

FDR is False Detection Rate which is defined as a false positive to a total number of positive results. FDR can be calculated using eq (5)

$$FDR = FP / (FP + TP) \quad (5)$$

The comparison of the proposed work with Almas et al., Rafeh et al., and Jamshidi et al. in terms of FDR is shown in Table 2 and Fig. 4.

Sybil nodes in network (in Percentage)	Almas et al.	Rafeh et al.	Jamshidi et al.	RTBSAD
10	10	12	15	2
20	15	17	20	5
30	17	20	22	10
40	19	22	25	12
50	25	26	28	15
60	30	35	40	20

Table 2: Comparison of RTBSAD with existing techniques in terms of FDR (in percentage)

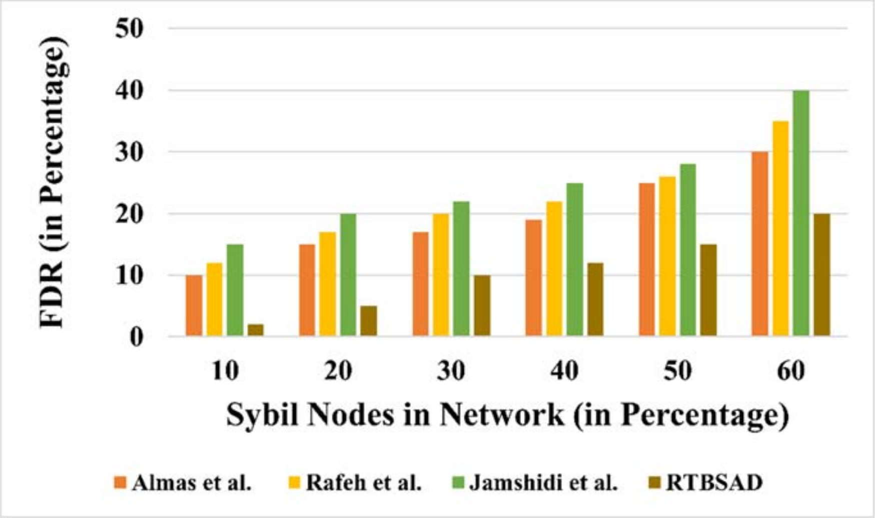

Fig. 4. The graphical representation of FDR results of proposed schemes with existing schemes

4.3. Average Energy Consumption

It refers to the total energy used by all nodes about total nodes. You can calculate it using Eq (6)

$$Average\ Energy\ Consumption = \frac{\sum_{i=1}^{N}(Initial_{energy} - node(i).energy)}{N} \quad (6)$$

Where N is the total number of nodes of a network. The comparison of the results of Average Energy Consumption is shown in Table 3 and Fig. 5.

Number of nodes in network	Almas et al.	Rafeh et al.	Jamshidi et al.	RTBSAD
100	3.2	3.4	3.5	2.7
150	3.5	3.7	3.8	2.8
200	3.8	3.9	4	3.2
250	4.2	4.2	4.3	3.3
300	4.3	4.3	4.5	3.8
350	4.4	4.5	4.6	4.1
400	4.7	4.8	4.9	4.2

Table 3: Comparison of RTBSAD with existing techniques in terms of Average energy consumed

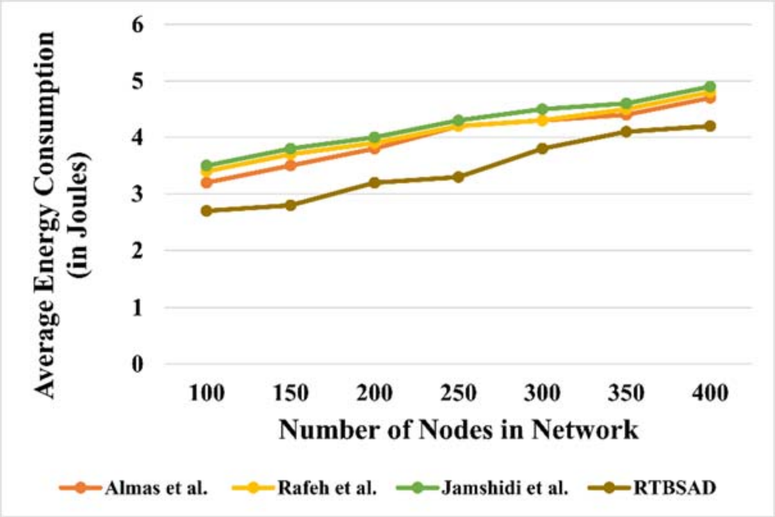

Fig. 5. Average Energy Consumption with varying number of nodes

4.4. Packet Delivery Ratio (PDR)

PDR is defined as the ratio of packets reached at the destination to the total number of packets forwarded. Higher PDR indicates the reliability of the network. The comparison of the PDR of the network with existing techniques is shown in Tab. 4. The graphical representation of Table 4 is shown in Fig. 6.

Sybil nodes in network (in Percentage)	Almas et al.	Rafeh et al.	Jamshidi et al.	RTBSAD
10	0.93	0.91	0.89	0.98
20	0.86	0.83	0.8	0.91
30	0.7	0.65	0.61	0.8
40	0.58	0.52	0.5	0.72
50	0.46	0.39	0.35	0.57
60	0.35	0.33	0.31	0.49

Table 4: Comparison of RTBSAD with existing techniques in terms of Packet Delivery Ratio (PDR)

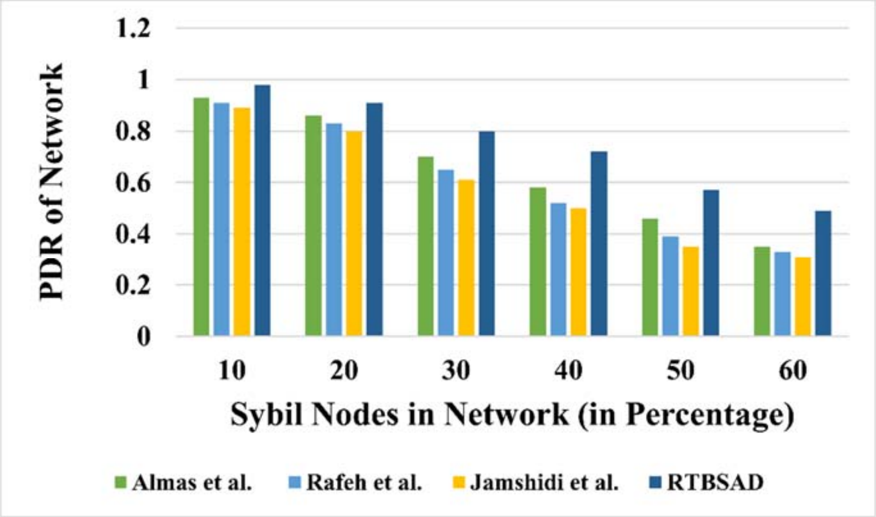

Fig. 6. PDR of network on a varying percentage of malicious nodes

It can be observed in Fig. 3, Fig. 4, Fig. 5 and Fig. 6 that the proposed scheme is better than Almas et al., Rafeh et al. and Jamshidi et al. in terms of TDR, FDR, Average Energy Consumed and PDR.

5. Conclusion

The number of devices connected to networks is growing with the advancement of technology and network. The passage of sensitive information through networks needs high security of sensor networks. But in the case of a Sybil attack, one can steal the identity of a legitimate node or can place Sybil nodes by forging fake identities. These Sybil nodes can affect routing, voting, data aggression, etc. The detection and prevention of Sybil nodes are extremely necessary for the smooth working of the network. In the present study RSSI and trust-based, Sybil attack detection model (RTBSAD) is proposed. This model is composed of two layers. In the first layer, RSSI value of a node is observed. Based on RSSI value nodes are distinguished into legitimate or Sybil nodes. To reduce false positives the threshold value of RSSI value is kept high and nodes that are left undetected in the first layer are detected in the second layer. The second layer of the algorithm consists of the trust model. To avoid Sybil nodes' bad mouthing, the trust model is built using direct and indirect trust. Comparing the proposed scheme with other techniques shows that proposed technique is superior in terms of TDR and FDR, Average energy consumption, PDR, and TDR. We plan to modify RTBSAD in the future to make it work on IoT-based applications.

Conflicts of Interest - The authors have no conflicts of interest to declare.

Acknowledgments

Meena Bharti would like to thank I.K. Gujral Punjab Technical University for offering the Ph.D. course in Computer Science & Engineering and providing support to access the resources for research.

References

[1] Abbas, S.; Merabti, M.; & Llewellyn-Jones, D. (2009). Signal strength-based Sybil attack detection in wireless Ad Hoc networks. *In Second International Conference on Developments in ESystems Engineering*, 190–195.

[2] Abbas, S.; Merabti, M.; Llewellyn-Jones, D.; & Kifayat, K. (2012). Lightweight sybil attack detection in manets. *IEEE Systems Journal*, *7*(2), 236–248.

[3] Almas Shehni, R.; Faez, K.; Eshghi, F.; & Kelarestaghi, M. (2018). A new lightweight watchdog-based algorithm for detecting Sybil nodes in mobile WSNs. *Future Internet*, *10*(1), 1.

[4] Alsaedi, N.; Hashim, F.; Sali, A.; & Rokhani, F. Z. (2017). Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS). *Computer Communications*, *110*, 75–82.

[5] Bali, R. S.; & Kumar, N. (2016). Secure clustering for efficient data dissemination in vehicular cyber–physical systems. *Future Generation Computer Systems*, *56*, 476–492.

[6] Bettstetter, C.; Resta, G.; & Santi, P. (2003). The node distribution of the random waypoint mobility model for wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, *2*(3), 257–269.

[7] Bhise, A. M.; & Kamble, S. D. (2016). Review on detection and mitigation of Sybil attack in the network. *Procedia Computer Science*, *78*, 395–401.

[8] Boukerch, A.; Xu, L.; & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, *30*(11–12), 2413–2427.

[9] Capkun, S.; Hubaux, J.-P.; & Buttyan, L. (2005). Mobility helps peer-to-peer security. *IEEE Transactions on Mobile Computing*, *5*(1), 43–51.

[10] Chakeres, I. D.; & Belding-Royer, E. M. (2004). AODV routing protocol implementation design. *In 24th International Conference on Distributed Computing Systems Workshops (ICDCS 2004 Workshops)*, 698–703.

[11] D’Angelo, G.; Palmieri, F.; & Rampone, S. (2019). Detecting unfair recommendations in trust-based pervasive environments. *Information Sciences*, *486*, 31–51.

[12] Demirbas, M.; & Song, Y. (2006). An RSSI-based scheme for sybil attack detection in wireless sensor networks. *In International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM’06)*, 5 pp. – 570.

[13] Douceur, J. R. (2002). The sybil attack. *International Workshop on Peer-to-Peer Systems*, 251–260.

[14] Gay, D.; Levis, P.; Von Behren, R.; Welsh, M.; Brewer, E.; & Culler, D. (2003). The nesC language: A holistic approach to networked embedded systems. *Acm Sigplan Notices*, *38*(5), 1–11.

[15] Golle, P.; Greene, D.; & Staddon, J. (2004). Detecting and correcting malicious data in VANETs. *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, 29–37.

[16] Hill, J. L.; & Culler, D. E. (2002). Mica: A wireless platform for deeply embedded networks. *IEEE Micro*, *22*(6), 12–24.

[17] Jamshidi, M.; Ranjbari, M.; Esnaashari, M.; Qader, N. N.; & Meybodi, M. R. (2018). Sybil node detection in mobile wireless sensor networks using observer nodes. *JOIV: International Journal on Informatics Visualization*, *2*(3), 159–165.

[18] Kim, J. U.; Kang, M. J.; Yi, J. M.; & Noh, D. K. (2015). A simple but accurate estimation of residual energy for reliable WSN applications. *International Journal of Distributed Sensor Networks*, *11*(8), 107627.

[19] Liang, W.; Long, J.; Weng, T.-H.; Chen, X.; Li, K.-C.; & Zomaya, A. Y. (2019). TBRS: A trust based recommendation scheme for vehicular CPS network. *Future Generation Computer Systems*, *92*, 383–398.

[20] Newport, C.; Kotz, D.; Yuan, Y.; Gray, R. S.; Liu, J.; & Elliott, C. (2007). Experimental evaluation of wireless simulation assumptions. *Simulation*, *83*(9), 643–661.

[21] Newsome, J.; Shi, E.; Song, D.; & Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses. *In Third International Symposium on Information Processing in Sensor Networks,* 259–268.

[22] Paul, A.; & Sinha, S. (2017). Performance analysis of received signal power-based Sybil detection in MANET using spline curve. *International Journal of Mobile Network Design and Innovation*, *7*(3–4), 222–232.

[23] Piro, C.; Shields, C.; & Levine, B. N. (2006). Detecting the sybil attack in mobile ad hoc networks. *In Securecomm and Workshops*, 1–11.

[24] Priyadarshi, R.; Rawat, P.; & Nath, V. (2019). Energy dependent cluster formation in heterogeneous wireless sensor network. *Microsystem Technologies*, *25*(6), 2313–2321.

[25] Rafeh, R.; & Khodadadi, M. (2014). Detecting sybil nodes in wireless sensor networks using two-hop messages. *Indian Journal of Science and Technology*, *7*(9), 1359–1368.

[26] Shah, P.; & Kasbe, T. (2021). Detecting Sybil Attack, Black Hole Attack and DoS Attack in VANET Using RSA Algorithm. *2021 Emerging Trends in Industry 4.0 (ETI 4.0)*, 1–7.

[27] Sun, Y.; & Zhao, Y. (2019). Dynamic adaptive trust management system in wireless sensor networks. *In 2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, 629–633.

[28] Wang, J.; Yang, G.; Sun, Y.; & Chen, S. (2007). Sybil attack detection based on RSSI for wireless sensor network. *In 2007 International Conference on Wireless Communications, Networking and Mobile Computing*, 2684–2687.

[29] Wu, B.; Chen, J.; Wu, J.; & Cardei, M. (2006). A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks. WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D. *Z. Du (Eds.)*.

[30] Xie, D.; Zhou, Q.; You, X.; Li, B.; & Yuan, X. (2013). A novel energy-efficient cluster formation strategy: From the perspective of cluster members. *IEEE Communications Letters*, *17*(11), 2044–2047.

[31] Yao, Y.; Xiao, B.; Wu, G.; Liu, X.; Yu, Z.; Zhang, K.; & Zhou, X. (2017). Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs. *In 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 591–602.

[32] Yao, Y.; Xiao, B.; Wu, G.; Liu, X.; Yu, Z.; Zhang, K.; & Zhou, X. (2018). Multi-channel based Sybil attack detection in vehicular ad hoc networks using RSSI. *IEEE Transactions on Mobile Computing*, *18*(2), 362–375.

[33] Zheng, J.; Bhuiyan, M. Z. A.; Liang, S.; Xing, X.; & Wang, G. (2014). Auction-based adaptive sensor activation algorithm for target tracking in wireless sensor networks. *Future Generation Computer Systems*, *39*, 88–99.

[34] Zhong, S.; Li, L.; Liu, Y. G.; & Yang, Y. R. (2004). Privacy-preserving location-based services for mobile users in wireless networks. *Department of Computer Science, Yale University, Technical Report ALEU/DCS/TR-1297*.

[35] Zhou, G.; He, T.; Krishnamurthy, S.; & Stankovic, J. A. (2004). Impact of radio irregularity on wireless sensor networks. *In Second International Conference on Mobile Systems, Applications, and Services (MobiSys2004)*.

Authors Profile

Meena Bharti is pursuing her Ph.D. in Computer Science and Engineering at I. K. Gujral Punjab Technical University, Kapurthala. She did her Bachelor of Technology in Computer Science and Engineering from MIMIT, Malout. She did her Master of Technology with in Software Engineering from Thapar University, Patiala. Her major area of research is Network security. Her area of interest is Network Security, OCR and Intrusion detection.
Email-id:meenabharti89@gmail.com

Dr. Shaveta Rani received her B.Tech. in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, India in 1998 and M.S. in Software Systems from Birla Institute of Technology and Science (BITS), Pilani, Rajsathan, India, in 2002. She did Ph.D. in Computer Science and Engineering from the Birla Institute of Technology and Science (BITS), Pilani, India, in 2009. Her Ph.D. thesis was "Investigations on Survivability Strategies in WDM Optical Networks". She worked in Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab, India as a Lecturer in the Department of Computer Science and Engineering from August 1998 to May 2005, as an Assistant Professor from May 2005 to May 2008, as Associate Professor from May 2008 to May 2011 and presently, since May 2011 she is working as Professor in the Department of Computer Science and Engineering in the same college. She has published many papers in refereed journals, chapters, books and conference proceedings on her research areas.
Email-id: garg_shavy@mrsptu.ac.in

Dr. Paramjeet Singh received his B.Tech. in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, India in 1998 and M.S. in Software Systems from Birla Institute of Technology and Science (BITS), Pilani, Rajsathan, India, in 2002. He did Ph.D. in Computer Science and Engineering from the Birla Institute of Technology and Science (BITS), Pilani, India, in 2009. His Ph.D. thesis was "Investigations on Routing and Wavelength Assignment Algorithms in WDM Optical Networks". He worked in Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab, India as Lecturer in the Department of Computer Science and Engineering from September 1998 to May 2005, as an Assistant Professor from May 2005 to May 2008, as Associate Professor from May 2008 to May 2011 and presently, since May 2011 he is working as Professor in the Department of Computer Science and Engineering in the same college. He also worked as HoD in the Department of Computer Science and Engineering of Giani Zail Singh College of Engineering and Technology, Bathinda, Punjab, India from December 2006 to March 2010. He has published many papers in refereed journals, chapters, books and conference proceedings on his research areas.
Email-id: param2009@mrsptu.ac.in