Published Online 18-03-2021

TRUST COMPUTATION USING BOTTOM-UP PARSER APPROACH IN MANET

Dr. S. Varalakshmi[1] ,Dr. A. Karthikayen[2] ,Dr. N.Satheesh kumar[3] ,Dr. S. Sankara Gomathi[4]

[1]Associate professor, Adhi College of Engineering and Technology, drssvlakshmi@gmail.com
[2]Professor, Visvodaya Engineering College, AP, akarthi_mathi@yahoo.co.in
[3]Professor, PBR Visvodaya Institute of Technology and Science, AP, sateeshkumar.n@visvodayata.ac.in
[3]Professor, Adhi College of Engineering and Technology, Chennai, ssgomathi@gmail.com

Abstract

In Mobile Ad hoc NETwork (MANET), the nodes are able to move from one point to other freely since it is a decentralized network. The objective of the proposed scheme is to remove the malicious nodes and to select the highly trusted nodes for transmitting the data. The node entering in to the network is checked for its identity either it is malicious or normal by applying bottom-up parser approach. The node is checked for their trust levels by using shift reduce operations which protects the sensed information from the malevolent node in the network. Therefore, the trusted source node sends the confidential data to the sink through the trusted nodes in the network. The simulation analysis is carried to prove the efficiency of the proposed scheme.

Keywords*: Trust Computation; Bottom-Up Parser; Shift-Reduce; Context Free Grammar; MANET*

I. Introduction

MANET refers to a unique type of wireless network, whereas nodes can travel independently with self-organizing capabilities. MANET owns its active characteristics because of node mobility. Also the network can be created to do some particular tasks and can be vanished in some interval of time since it has decentralized architecture [1]. Here decentralized denotes the network works without any background support like base station or gateway. Several routing algorithms have been proposed to improve the routing efficiency due to dynamic topology [2].

MANET includes a wide range of safety related applications like military communications, patient health care monitoring, etc. Due to the nature of broadcast wireless medium and decentralized architecture several routing conventions are vulnerable to attacks [3]. To ensure timeliness events in mobile wireless networks, a supportive event of packet-forwarding approach is applied. However, individual node’s coordination considered to be a difficult task while encouraging the other nodes for packet forwarding process. Reputation for each node is carried out in several ways for providing secured communication [4]. This implies that the throughput performance in MANET eventually increases. Cooperative packet forwarding schemes gets adjusted to other protocols without any QoS compromises. However, conventional packet forwarding schemes have limitations in the malicious node detection design [5].

II. Related Works

Security recently becomes a primary concern in order to provide protected communication between mobile nodes in an antagonistic environment. Compared to wire network the unique characteristics of MANET pose several nontrivial challenges in security design for highly dynamic network topology [6]. Angle and Context Free Grammar (ACFG) [7] were proposed to eliminate precarious node and to improve safety measure for MANETs. Here Elliptic Curve Cryptography (ECC) algorithm is applied for isolation of malevolent nodes. Intrusion Detection Systems (IDSs) was proposed in [8] comprises a new Cluster Head (CH) selection process. CH selection process is done based on Vickrey–Clarke–Groves mechanism which offers the intrusion detection service. Lightweight module and anomaly based heavyweight module are both combined to form a hybrid IDS. Primarily, the lightweight module is activated. The heavyweight module is used to intrusion detection process. Neighbor Detection Mechanism (NDM) [9] proposed to a common detection mechanism against neighbor attack in MANET.

Security Selection Scheme (SSS) for every data packet and security management seems to be a cost effective process [10]. The scheme named Authenticated Anonymous Secure Routing (AASR) [11] was proposed to protect the network from vigorous attacks. Onion routing is followed along with key-encryption mechanism therefore a verification message for routes prevent the nodes from avoiding false impression. The detection

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

process is analyzed using the entropy-defined trust model [12].

Node Reputation based Energy Aware Routing (NREAR) scheme [13] was proposed. The NREAR scheme is carried out with two phases like node behavior monitoring and node's energy value monitoring. First phase includes identification of belief nodes with the help of node behaviors (optimistic and pessimistic). Second phase calculates the energy value of the trusted (optimistic) nodes thereby data is passed over the optimistic nodes. An Intelligent Packet Forwarding Approach with Trust Model (IPFATM) based on the game theory [14] was proposed here trust evaluation plays a vital role in terms of node reputation aspect. The approach enforces an incentive modeling to carry the cooperation procedure between mobile nodes. Trust-based game increases the utility of packet-forwarding strategy.

III. Proposed Method

Trust Computation using Bottom Up Parser Approach (TCBUPA) scheme is proposed to improve the safety measures in MANET. The trusted nodes and the malicious nodes are detected by applying bottom-up parser method. Sender node needs to transmit the sensed information to the destination node if sink node not in the communication range of source node, then the control hello() message is passed over the neighbor nodes and it is passed towards the destination. The hello() message contains Src Id, String, Dest Id, relay_node ID. String assembly is done on basis of rightmost derivation.

a. Rightmost Derivation

The rightmost derivation is obtained by applying production to the rightmost variable and gets the string in each step. In each step the variable is replaced by its preceded value.

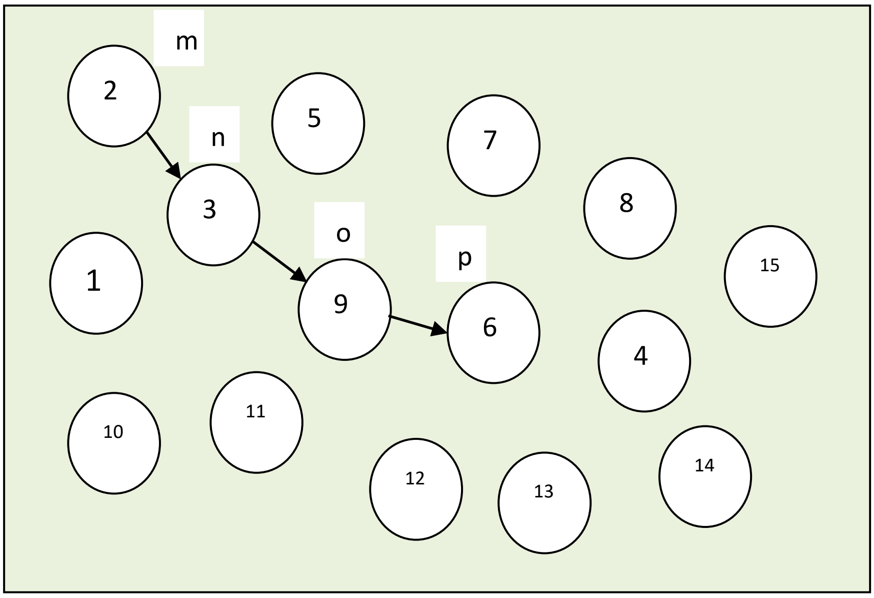

Figure 1: Example Network Scenario - TCBUPA

To verify the node trustworthiness s set of recursive rules for generating string pattern context free grammars is used. Figure 1 depicts the example scenario of the proposed scheme TCBUPA. Assume '2' as source node '3' and '9' as intermediate nodes and '6' as the destination node. Node 1 is source node '2' '3' and '4' are intermediate nodes, and 5 is destination node. Let node 1 holds terminal value of p, nodes '3' and '9' holds terminal values of q and r respectively and node 6 hold terminal value of s. Thereby the source and relay nodes are formed with rightmost derivation and it is given in equation 1. Let us consider the context free grammar (G) for the rightmost derivation,

$$G = (\{S\},\{m,n,o,p,\}P,S)$$

$$P = \{S \rightarrow S+S, S \rightarrow S*S, S \rightarrow S-S, S \rightarrow m, S \rightarrow n, S \rightarrow o, S \rightarrow p\} \quad (1)$$

Now the source node terminal '1' and intermediate terminals are formed with the rightmost derivation using the grammar rules and it is given in equation 2.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

$$S\overset{RM}{\Rightarrow}S*S\overset{RM}{\Rightarrow}S*p\overset{RM}{\Rightarrow}S-S*\mathrm{p}\overset{RM}{\Rightarrow}S-o*p\Rightarrow S\overset{RM}{\Rightarrow}S+n-o*p\overset{RM}{\Rightarrow}S\overset{RM}{\Rightarrow}m+n-o*p\} \qquad (2)$$

The trusted nodes are collected through the rightmost derivation or bottom-up parser method, the reliable nodes with minimum hop count is selected for optimal data routing. The trusted nodes store their terminal string value in a board. Then the source checks this string using shift reduce operation. If source node gets null string, then the nodes presented in the route are considered to be trusted nodes else the route is considered as malicious and the data transmission process is stopped with the notification message.

b. Bottom-Up Parser

In general the parsing technique quickly identifies the error or any conductance of misbehavior action. Therefore bottom-up parser approach is used here to identify the malicious nodes quickly and accurately. This bottom-up parser procedure mainly done with four operations such as move, reduce, fault and agree. In move function, the upcoming input symbol is moved to the bottom of the load. In reduce operation; the string is placed at the position of the stack.

The stack 'S' should be relocated and to be decided with what terminal to be replaced with the string. In agree procedure, the parser operation is done successfully and in fault action, the parser reveals the erroneous part and an error recovery procedure is called out. The routing nodes 2, 3, 9 and 6 holds the terminal values of m, n, o and p and formed the string. In order to verify the node trustworthiness present in the route, the source node verifies the string series using bottom-up parser.

Table 1: Bottom-Up Parser

Stack	Input buffer	Transition
$	m+n*o-p$	Move
$m	+n*o-p$	Reduce(S→m)
$S	+n*o-p$	Move
$S+	n*o-p$	Move
$S+n	*o-p$	Reduce(S→n)
$S+S	*o-p$	Reduce(S→S+S)
$S	*o-p$	Move
$S*	o-p$	Move
$S*o	-p$	Reduce(S→o)
$S*S	-p$	Reduce(S→S*S)
$S	-p$	Move
$S-p	$	Reduce(S→p)
$S-S	$	Reduce(S→S)
$S	**$**	Allow

Bottom-Up Parser Algorithm

```
Terminal = following terminal()
Do proc()
   S = bottom of stack
   if proceed[S, terminal] = shift 'm' then
   Move 'm'
   label = following proc()
   else if proceed[m, label(n-o*p)] = reduce S= S+ then
   Add 2 + [S] signs
   S = bottom of stack
   Move n
   Move goto [n,S]
   else if proceed[k, string(0)] = "agree" then
   return proc()
   else;
   error()
```

Table 1 gives shift reduce parser (bottom-up parser) in detail. The source node gets empty string and nodes are verified to be trustworthy nodes. The routing path is allowed and the data transmission process can be carried out successfully through this route. The malicious node can be easily detected in the route if the string contains some non related values. Thereby the routing nodes in that particular path are rejected and identify which node performing malicious activities.

IV. Results and Discussion

Simulation of both proposed and existing schemes are carried out in a simulation tool called Network Simulator (NS). Packet Delivery Rate (PDR), Packet Loss Rate (PLR), Throughput and Detection rate are the simulation metrics used to evaluate the proposed scheme with the conventional protocol.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

PDR

The ratio of sensed packets that delivered effectively to the sink or receiver node is said to be packet delivered rate. The data bits are created by the CBR sources. Figure 2 shows the PDR of proposed and existing scheme and the graph clearly shows the proposed scheme has good delivery rates of packets at the receiver end. It is evaluated through the equation 3 given below; here T denotes time and n denotes number of nodes.

$$PDR = \frac{\sum_{0}^{n} Pkts\,Delivered}{T} \tag{3}$$

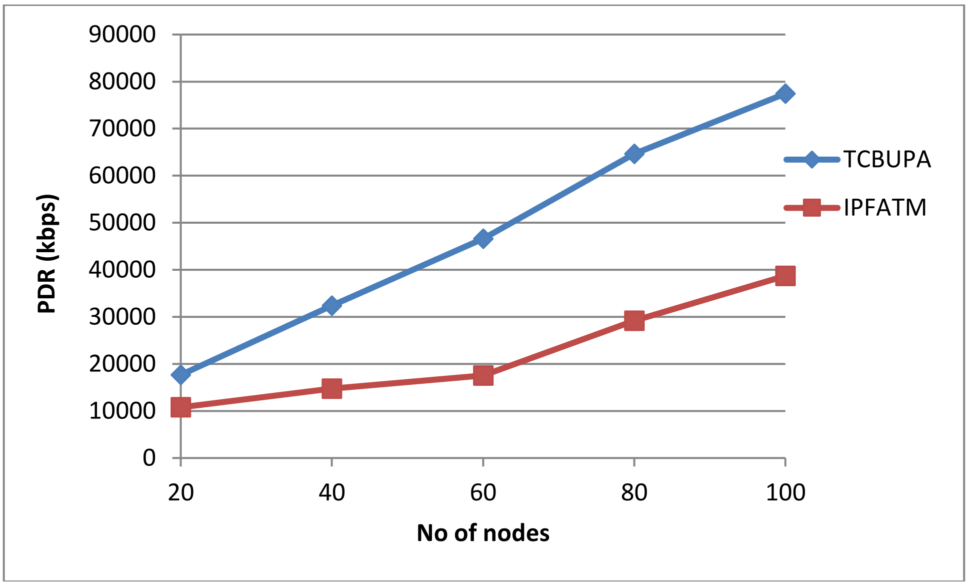

Figure 2: PDR

PLR

Number of data packets that lost due to link failure or malicious activities of nodes. PLR is estimated by equation 4.

$$PLR = \frac{\sum_{0}^{n} Pkts\,Dropped}{T} \tag{4}$$

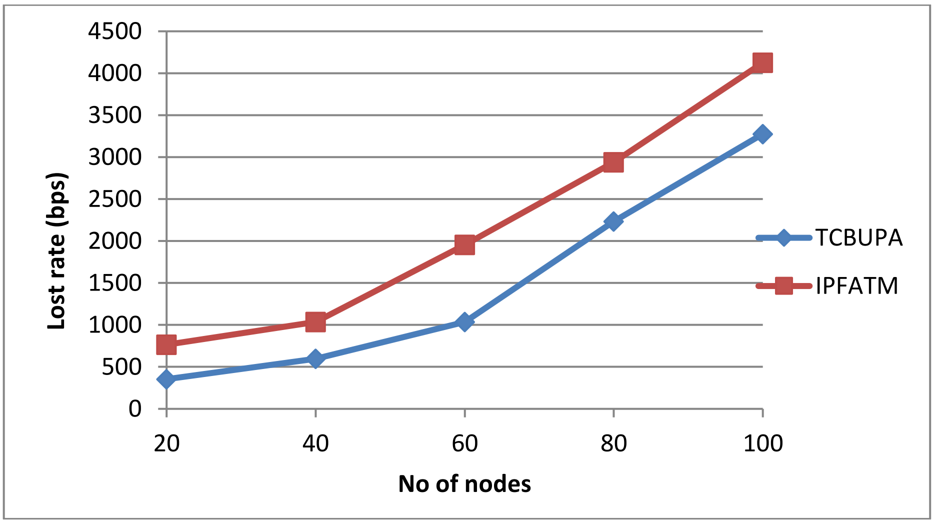

Figure 3: PLR

Figure 3 shows the graphical representation of loss rates for both proposed TCBUPA and conventional scheme IPFATM. Proposed scheme has low loss rate ratio compared to the existing scheme.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Throughput

The successful transmission of data packets over the network is said to be throughput and it is calculated with every packet sent respectively.

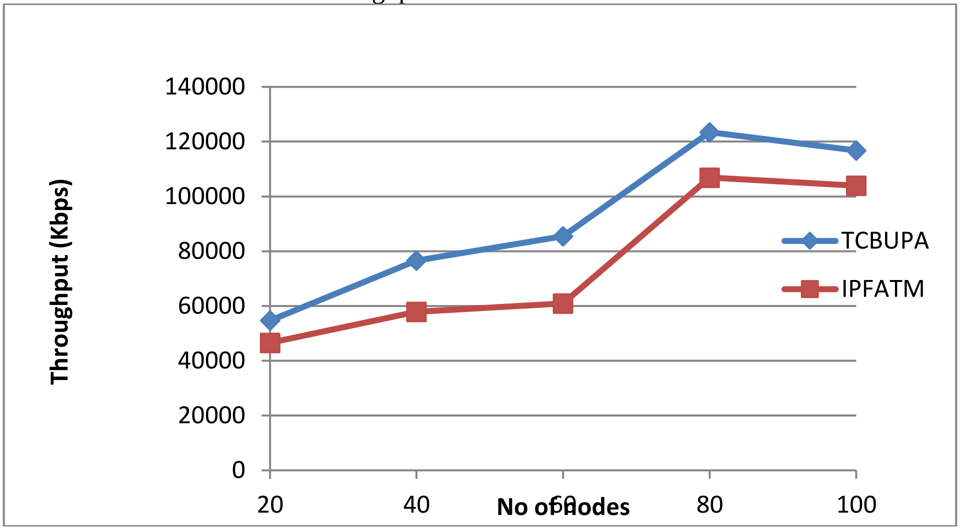

Figure 4: Throughput

Figure 4 shows the throughput variations achieved for both TCBUPA and IPFATM scheme. Proposed scheme TCBUPA achieves better network throughput. Equation 5 is used to estimate system throughput.

$$Throughput = \frac{\sum_0^n Pkts\ recvd\ (n) * Pkt\ size}{1000} \tag{5}$$

Detection Ratio

The nodes that fall under malicious category are defined to be detection ratio here. The malicious node detection ratio D_{RATIO} is calculated using equation 6.

$$D_{RATIO} = \frac{D_{mn}}{T_{Nn}} \tag{6}$$

where D_{mn} denotes malicious node count through the number of normal nodes (one or more than one), T_{Nn} is the total number of normal nodes.

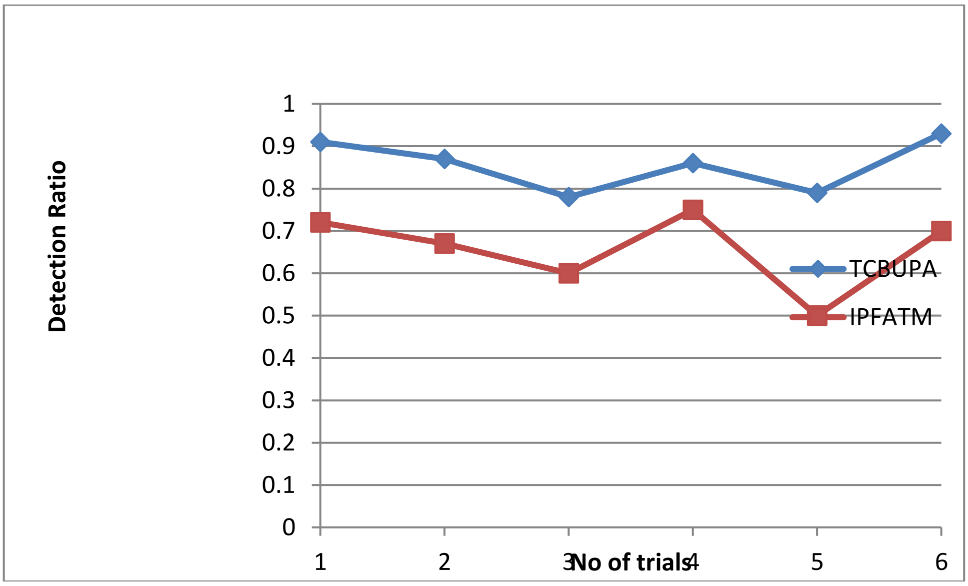

Figure 5: Detection Ratio

The proposed TCBUPA have high ability in detecting malicious nodes that present in the routing path compared to the conventional IPFATM scheme

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

and it is shown in figure 5.

V. Conclusion

The objective of this TCBUPA scheme is to remove the malicious nodes and to select the highly trusted nodes for transmitting the data. The node entering in to the network is checked for its identity either it is malicious or normal by applying bottom-up parser approach. The node is checked for their trust levels using rightmost deviation operations in order to safeguard the information from the malevolent node in the network. Therefore, the trusted source node sends the confidential data to the sink through the trusted nodes in the network. The simulation analysis is carried to prove the efficiency of the proposed scheme.

References

1. Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Najeeb, A. R., & Yaacob, M. (2018). A survey on MANETs: architecture, evolution, applications, security issues and solutions. Indonesian Journal of Electrical Engineering and Computer Science, 12(2), 832-842.

2. Kumar, S., Saini, M. L., & Kumar, S. (2018). A survey: swarm based routing algorithm toward improved quality of service in MANET. Int J Manage Technol Eng, 8(5), 311-322.

3. Jamal, T., & Butt, S. A. (2019). Malicious node analysis in MANETS. *International Journal of Information Technology*, *11*(4), 859-867.

4. Almazyad, A. S. (2018). Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks. *Neural Computing and Applications*, *29*(9), 597-607.

5. Bisen, D., & Sharma, S. (2018). Fuzzy based detection of malicious activity for security assessment of MANET. *National Academy science letters*, *41*(1), 23-28.

6. Kumar, A. S., & Logashanmugam, E. (2014, July). To enhance security scheme for MANET using HMAC. In *Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014* (pp. 467-471). IEEE.

7. Veerasamy, A., Madane, S. R., Sivakumar, K., & Sivaraman, A. (2016). Angle and context free grammar based precarious node detection and secure data transmission in MANETs. *The Scientific World Journal*, *2016*.

8. Subba, B., Biswas, S., & Karmakar, S. (2016). Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. *Engineering Science and Technology, an International Journal*, *19*(2), 782-799.

9. S. Parthiban, A. Amuthan, N.Shanmugam, K.Suresh Joseph, Neighbor Attack And Detection mechanism In Mobile Ad-Hoc Networks, Advanced Computing: An International Journal, Vol.3, No.2, March 2012.

10. M. Saleh and L. Dong, “Real-time scheduling with security enhancement for packet switched networks,” *IEEE Transactions on Network and ServiceManagement*, vol. 10, no. 3, pp. 271–285, 2013.

11. W. Liu and M. Yu, “AASR: authenticated anonymous secure routing for MANETs in adversarial environments,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4585–4593, 2014.

12. M. Abdelhakim, L. E. Lightfoot, J. Ren, and T. Li, “Distributed detection in mobile access wireless sensor networks under byzantine attacks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 4, pp. 950–959, 2014.

13. Thirunavukkarasu, V., Kumar, A. S., Josephine, D. J., & Arasu, T. P. (2020, July). Selection of Optimistic Nodes for Reputation Based Routing in Wireless Networks. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-5). IEEE.

14. Khan, B. U. I., Anwar, F., Olanrewaju, R. F., Pampori, B. R., & Mir, R. N. (2020). A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission With Optimized Network Operations in Futuristic Mobile Adhoc Networks. IEEE Access, 8, 124097-124109.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731