Hindawi Publishing Corporation
The Scientific World Journal
Volume 2016, Article ID 3596345, 12 pages
http://dx.doi.org/10.1155/2016/3596345

Research Article

Angle and Context Free Grammar Based Precarious Node Detection and Secure Data Transmission in MANETs

Anitha Veerasamy,[1] Srinivasa Rao Madane,[2] K. Sivakumar,[3] and Audithan Sivaraman[4]

[1]*Department of Information Technology, Anna University, Chennai, Tamil Nadu 600025, India*
[2]*Department of Computer Science and Engineering, Adhiparasakthi College of Engineering, Vellore, Tamil Nadu 603319, India*
[3]*Department of Computer Science, College of Computer Science, King Khalid University, Abha 62529, Saudi Arabia*
[4]*Department of Electronics and Communication Engineering, PRIST University, Thanjavur, Tamil Nadu 613403, India*

Correspondence should be addressed to Anitha Veerasamy; anithav.annauniv@gmail.com

Received 5 August 2015; Accepted 12 November 2015

Academic Editor: Juan M. Corchado

Growing attractiveness of Mobile Ad Hoc Networks (MANETs), its features, and usage has led to the launching of threats and attacks to bring negative consequences in the society. The typical features of MANETs, especially with dynamic topology and open wireless medium, may leave MANETs vulnerable. Trust management using uncertain reasoning scheme has previously attempted to solve this problem. However, it produces additional overhead while securing the network. Hence, a Location and Trust-based secure communication scheme (L&TS) is proposed to overcome this limitation. Since the design securing requires more than two data algorithms, the cost of the system goes up. Another mechanism proposed in this paper, Angle and Context Free Grammar (ACFG) based precarious node elimination and secure communication in MANETs, intends to secure data transmission and detect precarious nodes in a MANET at a comparatively lower cost. The Elliptic Curve function is used to isolate a malicious node, thereby incorporating secure data transfer. Simulation results show that the dynamic estimation of the metrics improves throughput by 26% in L&TS when compared to the TMUR. ACFG achieves 33% and 51% throughput increase when compared to L&TS and TMUR mechanisms, respectively.

1. Introduction

Mobile Ad Hoc Networks (MANETs) embrace various computational nodes that can communicate with one another within a specified wireless range. The most favoured feature of MANETs is their capability to allow communication during node mobility. However, the shared wireless medium of MANET facilitates inactive and adversarial eavesdropping on data communications, where adversaries can start various overwhelming attack on the network. Many protocols have been designed for protecting the wireless communication but do not grant significance in privacy protection and leave mobile nodes to be noticeable by wireless analysis. Secure data transmission in MANET is thus a very challenging task. An example MANET is shown in Figure 1.

To overcome this problem, two strategies are proposed and evaluated in this paper, Location and Trust-based secure communication scheme (L&TS) and Angle and Context Free Grammar (ACFG) based precarious node detection and secure communication in MANETS.

Firstly, a Location and Trust-based secure communication scheme assigns algorithms for data integrity based on how far the nodes are located from one another. The next hop is selected based on the trust. A trust value is calculated based on the previous network operations for effective next hop selection, which makes this scheme work efficiently even under high mobility conditions. A design limitation identified in this scheme has motivated us in the design of ACFG scheme for MANETs.

In ACFG scheme, the next hop is selected based on a node's angle and a node's left most and right most derivations. There are three levels of assessment: first the node's location is assessed using the angle method, followed by the CFG to detect which node among the neighbors has

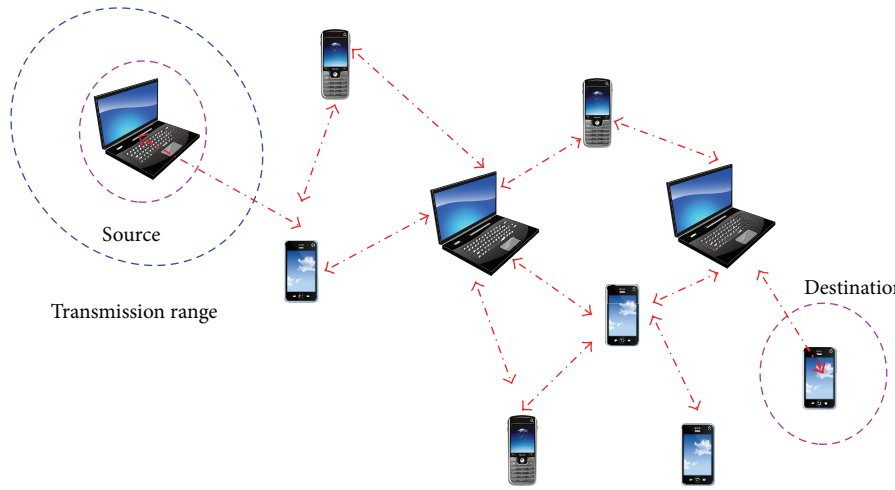

Figure 1: Mobile Ad Hoc Networks.

faked the location; the last confirmation using an elliptic cryptography function is achieved to publish that a node is malicious. In this scheme, there is no requirement for extraordinary nodes for the localization process or for other special purposes. Hence, it provides better performance when compared to L&TS mechanism. The organization of the paper is, thus, related works following Introduction, the proposed methods, and simulation analysis.

2. Related Work

The works related to the mechanism proposed here are broadly classified based on security, location, and Angle and Context Free Grammar (CFG) used as estimation parameters while routing.

2.1. Security. Many protocols have improved security using different aspects in the literature. The ad hoc networks are classified into three types: open, managed-open, and managed-hostile, dissimilar in the safety requirement. SPAAR is one protocol that aims to provide security in a *managed-hostile* environment, which is described as a MANET created using military nodes in a battle situation [1]. Secure Routing Protocol (SRP) [2], on the other hand, needs a security association across end nodes assuring that they can differentiate and drop reply messages giving any fake information or even stop receiving the same. This is achieved by employing and using a shared secret to the main routing protocol, for example, AODV. The trust based routing protocols [3, 4] are assigned trusted values and the data are routed only through trusted nodes.

Selection of security scheme for every data packet and management of the same is a tedious and expensive process [5]. In the Authenticated Anonymous Secure Routing (AASR) [6] the RREQ packets are legitimated using group signatures and to preserve vigorous attacks from unveiling the node distinctiveness. The key-encrypted onion routing containing a route secret verification message prevents the nodes from avoiding misinterpretation of a genuine intention. Provision of high anonymity and security is considered an advantage. However, there is enormous packet delay during data transmission. The sensors' decision reports are used to discover the malicious nodes and estimate their attack behaviour. The detection procedure is analyzed using the entropy-defined trust model [7].

2.2. Location. Localization verification technique [8] depends on the received signal strength. A node confirms the truthfulness of the other node by predicting its next geographical localizations and checks the similarity to the actual localizations found. A node confirms the truthfulness of the other node by predicting its next geographical localizations and checks the similarity to the actual localizations found in Efficient Mobility Based Localization (EMBL) [9]. During the localization method, each node predicts its future mobility pattern according to its past known location information. However, there is poor accuracy in predicting the real and estimated node positions, and distances from a reference node. Ordinary nodes among anchor nodes and unknown nodes build a shortest path by greedy approach [10]. This shortest path is approximately a straight line between unknown nodes and reference nodes. The disadvantage of this algorithm is the poor accuracy when there are too many routers.

In Modified Parametric Location Identification (MPLI) [11], location is identified separately using the x and y coordinates, angle of arrival, time, distance, and circular region quadrants. It also provides timely updates of positions to make the routing more robust and position aware to avoid data losses and connection termination due to mobility. Multihop Localization Algorithm (MLA) [12] has five steps as follows: (1) achieving neighbor distances, (2) calculating reference node distances (unidentified nodes can estimate the total distances to nodes with the data obtained from step 1, and they decide the shortest paths to anchor), (3) choosing the reference nodes, (4) acquiring angles, and (5) fitting the shortest path to straight line.

2.3. Angle. Decoupled Maximum Likelihood (DEML) angle estimator determines the angle of arrival [13]. The DEML

estimator is no longer asymptotically statistically proficient. Angular Routing Protocol (ARP) [14] based on position that uses an improved geographic forwarding to route packets to the destination. The geographic forwarding fails, at a time used by the angle-based forwarding method. It does not require establishing routes. The indefinite node estimates its angle to each of the three reference nodes, based on these angles, and the positions of the reference nodes (that form a triangle), and computes its own position using simple trigonometrical relationships [15]. The triangular zone [16] is used to reduce the route searching space. This mechanism avoids huge routing traffic and collision.

The angle is found based on slope of line. Slope values are found in all neighboring nodes [17]. The angles between unidentified node and several fixed nodes are used in the AOA (angle of arrival) [18] to evaluate the position, which is a little costly to perform. Orthomorphic Analyst k-Nearest Neighbor method [19] detects the intrusion activity based on the traffic intensity at inner boundary instance within the communication MANETs. Angle based distance is measured between the node points for easy detection of traffic creating nodes. It measures how far each pair of mobile nodes is and evaluates correct angle of position within the inner boundary.

2.4. CFG. One-time authentication information [20] discussed structured and unstructured techniques for generating strings and analyses of the difficulty of guessing strings in such a language. This authentication information is used for the generation of one-time passwords. This one-time authentication information is still inclined to operate in the middle attacks. Probabilistic Context Free Grammars (PCFGs) [21] recognized events from raw sensor network measurements. It derived a brief probabilistic Context Free Grammar from the known examining data. A metric depending on Bayesian formula for maximizing grammar, a posteriori probability given the training data, is used here. Advantages of the properties are the chunk and merge operations.

Translate natural language sentence into database query NLDBI (Natural Language Interface to a Database) structure [22] including its probabilistic Context Free Grammar, it is used to construct the parse tree, and this algorithm calculates the probabilities. CFG has a formalization capability in describing most sentence structures and so well formed that efficient sentence parser.

Trust management system enhances the protection in MANETs [18]; the trust model has trust from direct and indirect observations. In direct observation, the trust value is derived using Bayesian inference; it is a type of uncertain reasoning where the full probability model can be defined. In indirect observation, the trust value is derived using the Dempster-Shafer theory; it is another type of uncertain reasoning where the proposition of interest can be derived.

This method separates data packets and control packets and mitigates factors that cause packet losses. After examination of the trust value, there is a possibility for the inside attackers to conquer the other nodes. In such a situation, the Location and Trust-based secure communication scheme is used to provide security in MANETs.

3. Location and Trust-Based Secure Communication Scheme (L&TS)

The proposed scheme provides a technique to manage and use different security schemes in a single MANET simultaneously. It uses the security algorithms available as security providers based on how far the nodes are located from the corresponding destination nodes. The security schemes are known in prior to the nodes operating in the MANET. Each node chooses its own security algorithm based on how far the destination is located and sends the data to the destination. This is performed with an understanding that the farthest nodes or the nodes that require multihop transmission require higher security than nodes that are closer to each other and are capable of direct transmission.

3.1. Working of the Scheme. The actual working of the scheme can be divided into the following processes: Data Collection, L&TS Management, Selection of Security Algorithm, and Data Transmission. The architectural working of the L&TS in MANETs is described in Figure 2.

3.1.1. Data Collection. Each node in the MANET sends a route request RREQ message along with the location information in order to transmit data to its destination. In return, it receives a route reply RREP message that also contains the location information of the destination. The information about the most recent transmissions for that node is collected from every node as well.

3.1.2. L&TS Management. An arbitrary manager called the L&TS manager processes the information collected. Based on the location information of the source and destination the distance between them is calculated dynamically and compared with threshold values th_1, th_2, and th_3 (in this case) and it can go up to th_i. The trust values $T(n)$ are also assigned based on the most recent transmissions.

3.1.3. Selection of Security Algorithm. A number of security algorithms (i.e., RSA + MD5; HMAC + MD5; and HMAC + SHA-1) are stored in a database and based on the comparison of the L&TS manager, a particular transmission is assigned Algorithm i. For example, if d value is less than th_1 then Algorithm 1 is selected; if it is less than th_2, then Algorithm 2 is selected, and so on up to Algorithm i. It is significant to mention that Algorithm 1 has lower security standard than Algorithm 2.

3.1.4. Data Transmission. The data transmission is carried out based on the trust values $T(n)$ of the nodes in the network through shortest path distance. If the source and destination are within the range of each other, then direct communication is performed. The threshold values are stable yet the mobility of the nodes alters the type of security algorithm used when the d value switches from one threshold value to another. This makes the transmission security switch from Algorithm 1 to Algorithm 2. This is a well-informed process so the destination alone knows which algorithm is used and when.

Figure 3 shows the Trusted Route obtained from the history of usage of a node for previous network operations. A

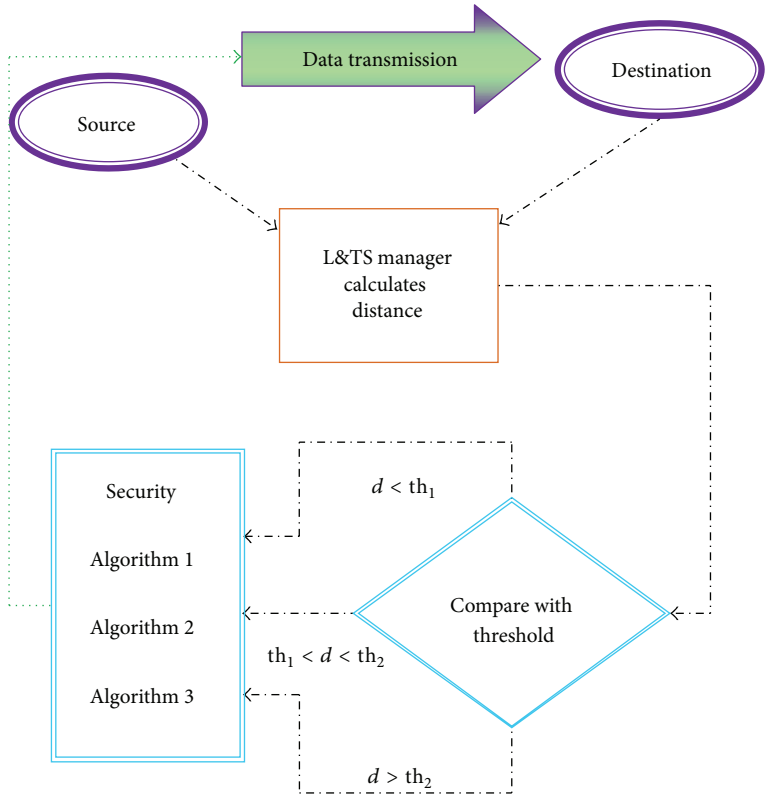

Figure 2: Working of the L&TS scheme.

node that is newly introduced into the MANETs is assigned an optimum history value H by authenticated persons. For a normal node, as the network operations are performed in the system, the value of $T(n)$ is incremented relatively by the nodes that communicate to it. If the quality of service (QoS) of the node is diminishing then the value of $T(n)$ is decremented. Based on the value of $T(n)$ at the instant i, the routing to the destination along with the selected security scheme is performed. Distrusted nodes are not preferred for the routing operations; this provides security during routing.

3.1.5. Result Notification. In this phase, the security is provided based on the destination location from the source. The trust value T is estimated from history of usage of previous network communication process. It works well under high mobility.

3.2. Limitation of L&TS. The forwarding node is selected based on the history of previous transmission. There exists a drawback in L&TS that has been identified in this section. The cost of this system is considerably high.

4. Angle and Context Free Grammar (ACFG) Based Precarious Node Detection and Secure Data Transmission

Trust management using uncertain reasoning method has higher delay and packet loss. Even after the evaluation of the trust value, there is a possibility for the insider attackers

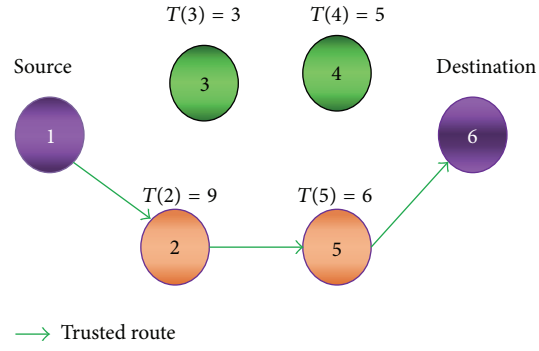

Figure 3: Trust route formation.

to ruin the nodes. Therefore, there is an absolute need to introduce a novel method to improve the security. Pertaining to this concern, an Angle and CFG based precarious node detection and secure data transmission mechanism is proposed in MANETs. In this scheme, the precarious node detection uses Angle and CFG method (Levels 1 and 2) and secure data transmission after publishing malicious nodes using Elliptic Curve Cryptography (Level-3).

4.1. Forwarding Node Selection. If a source node (S) likes to send a packet to the destination (D), the source selects a next hop (N) from its neighbor table. The next hop selects the closest node to the destination among the neighboring nodes of the source node. The next hop node is selected based on the minimum spanning tree shortest path algorithm.

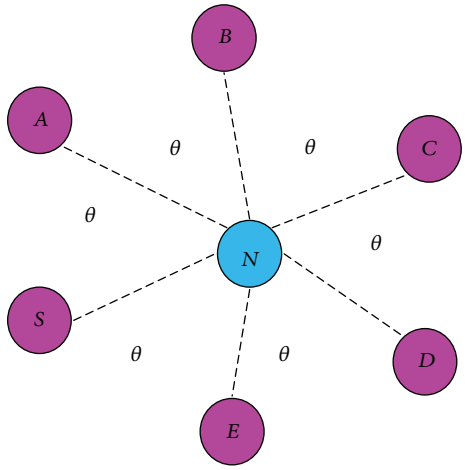

Figure 4: Next hop neighbor angle.

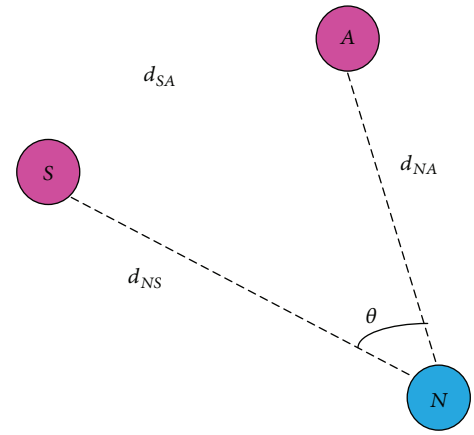

Figure 5: Individual neighbor angle.

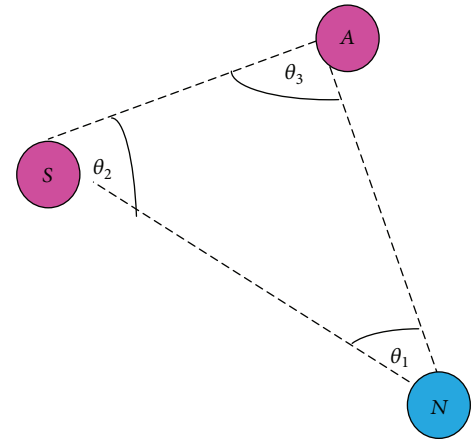

Figure 6: Interior angles.

4.2. Neighbor Angle Computation. The source selects the neighbor node N and collects their surrounding neighbor nodes and then computes the angles of the neighbor nodes.

Figure 4 shows that the node S is a source, N is a next hop node, and A, B, C, D, and E are node N's neighbors. Source collects the angles that node N makes with N's neighbors (shown as θ in Figure 4). Note that θ is an arbitrary value and varies from one node to another unlike in Figure 4.

Figure 5 shows the nodes S and A belonging to N's neighbor list. In triangle, the distance of d_{NS}, d_{SA}, and d_{NA} is obtained from the RSS values of the acknowledgement received from node S and node A. The angle $\angle SNA$ is represented as θ. The value of θ is computationally obtained by the equation given below in (2).

The distance is measured by

$$d = \sqrt{(x - x_1)^2 + (y - y_1)^2}, \tag{1}$$

where x_1 and x_2 are the coordinates of the two nodes between distances. The angle θ is calculated based on

$$\theta = \arccos\left[\frac{b^2 + c^2 - a^2}{2bc}\right], \tag{2}$$

where $a \rightarrow d_{SA}, b \rightarrow d_{NS}, c \rightarrow d_{NA}$.

Similarly, the algorithm computes every neighbor angle of the node N. The source stores every neighbor node angle in a table. Source S, next hop node N, common neighbor of S and N = node A form a triangle. The three interior angles are discovered and added up. Figure 6 shows that the θ_1, θ_2, and θ_3 are three interior angles. Mathematically, the addition of all three interior angles is 180°, where $\angle SNA = \theta_1$, $\angle ASN = \theta_2$, and $\angle NAS = \theta_3$:

$$\begin{aligned} \angle SNA + \angle ASN + \angle NAS &= 180^\circ, \\ \theta_1 + \theta_2 + \theta_3 &= 180^\circ. \end{aligned} \tag{3}$$

In Figure 5, the angle computed from the RSS for $\angle SNA = \theta$ replaces the interior angle $\angle SNA = \theta_1$. Now according to the property of a triangle,

$$\theta + \theta_2 + \theta_3 = 180^\circ. \tag{4}$$

If the sum of the angles in the expression (4) adds up to make 180 degrees, then the nodes that make up the triangle are proved to be legitimate nodes. Hence, the source selects the next hop node only if the node is legitimate according to this method. Otherwise, one among the three nodes forming the triangle is said to be faulty and Level 1 test fails here. The source needs to identify which node is a precarious node and for that a novel Context Free Grammar verification method is proposed in the following section.

4.3. CFG Based Node Verification. The CFG based node verification (Level 2 test) is only performed when the angle based detection mechanism detects a faulty node. Generally, all nodes of the network have a mapping variable. The Leftmost and Rightmost derivations are obtained based on this mapping variable. The source S computes the leftmost derivation and the next node N computes the rightmost derivation. Finally, the source checks whether these derivations are equal

```
(1)  Input Source S, Destination D, a new node N and Common Near node A
(2)  Output Legitimate Forwarder node
(3)  Begin procedure
(4)    While source not reach D do
(5)        Collect N neighbor node
(6)        Foreach neighbor node do
(7)            Neighbor angle θ
(8)        S, N, and A to form a triangle then
(9)        compute the interior angles of S, N, and A
(10)       θ1 + θ2 + θ3 = 180°
(11)       Replaced corresponding interior angle by the neighbor angle θ
(12)       θ + θ2 + θ3 = 180°
(13)       If θ == θ1 then
(14)           Select node is a N goto (4)
(15)       Else Let LM be the Leftmost Derivation
(16)           Let RM be the Rightmost Derivation
(17)           To compute LM and DM of S and N
(18)           If LM == RM then
(19)               Choose N is a Forward node goto (4)
(20)           Else To compute LM and RM of S and A
(21)               If LM == RM then
(22)                   Choose A is a Forward node goto (4)
(23)                   Else
(24)                       Set F ← Level3_ECC_Check()
(25)                       If F = 0 then
(26)                           Source select next near node N goto (1)
(27)                       Else To continue routing to same node and goto (4)
(28) End procedure
```

Algorithm 1

or not. If it is equal, then node is legitimate; otherwise, the node is precarious.

4.3.1. Leftmost and Rightmost Derivation. A leftmost derivation chooses the leftmost nonterminal to expand and the right most derivation chooses the rightmost nonterminals to expand. Every node is assigned a mapping function in the proposed system and the leftmost and rightmost derivations are obtained based on this mapping function.

In Figure 7, S is a source, N is a next hop, and A is a common node. Let node a be a mapping function of A, let n be a mapping function of N, and let s be a mapping function of S; these mapping functions will be applied to the CFG. The source checks nodes A and N, which node of left most and right most derivation is equal so that it can be selected as the next forwarding node. For example, the leftmost and rightmost derivation of nodes S and N is given below.

Consider Figure 7: the derivation is obtained among nodes S, A, and N. The mapping functions are s, a, and n. The leftmost and rightmost derivation between S and N is given below.

Given the grammar, $G = (\{S\}, \{s, n\}R, S)$.

Consider the grammar G with production:

$$R = \{S \longrightarrow sSSn, S \longrightarrow a, S \longrightarrow n, S \longrightarrow s\}. \quad (5)$$

The leftmost derivation of source and next hop is given below:

$$S \overset{\text{LM}}{\Longrightarrow} sSSn \overset{\text{LM}}{\Longrightarrow} ssSn \overset{\text{LM}}{\Longrightarrow} ssnn. \quad (6)$$

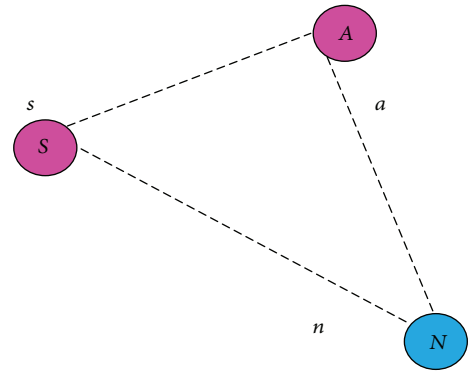

Figure 7: Mapping function.

Rightmost derivation of source and next hop is the following:

$$S \overset{\text{RM}}{\Longrightarrow} sSSn \overset{\text{RM}}{\Longrightarrow} sSnn \overset{\text{RM}}{\Longrightarrow} ssnn. \quad (7)$$

The leftmost derivation is obtained based on the mapping function and stores the string value in a table. Next node/common node is derived by the rightmost derivation. If the source checks leftmost and right most derivations are equals, that node is legitimate; otherwise it is a precarious node. The algorithm used to design the ACFG mechanism is given in Algorithm 1 that corresponds to the various steps illustrated in the flowchart of Figure 8.

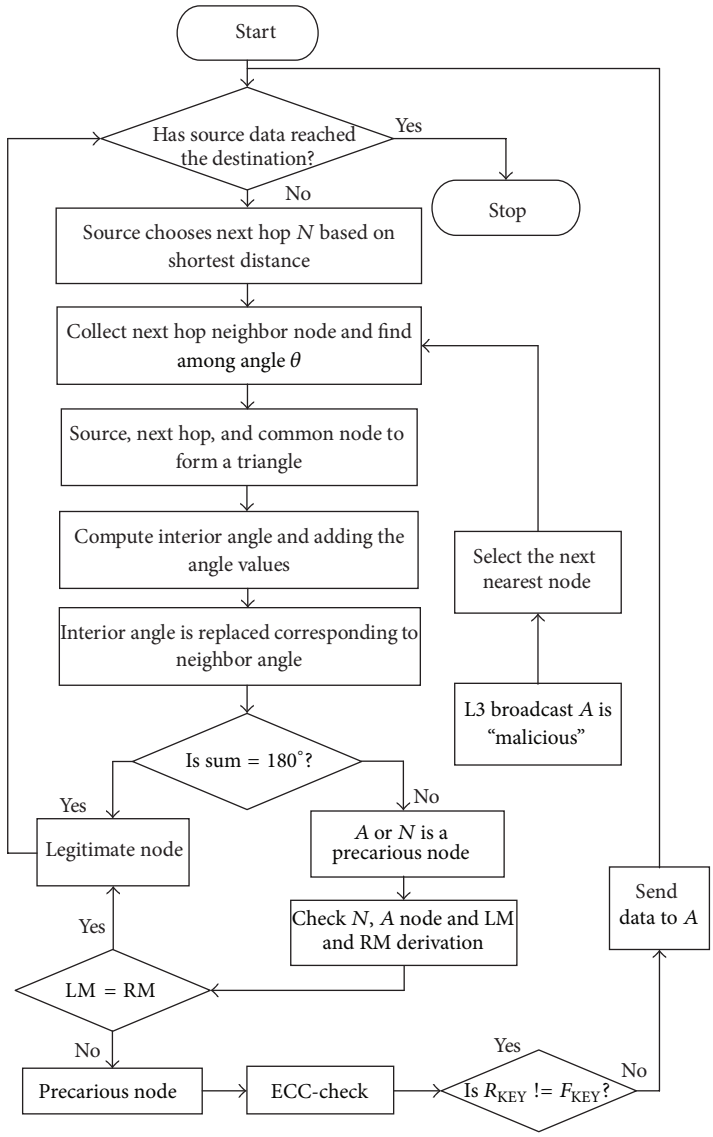

Figure 8: Flowchart of ACFG scheme.

4.4. Secure Data Transmission Using Reinforcement. The reinforcement action of this scheme is to publish that a node is malicious to all other nodes so that the node can be excluded from the communication process. This comes under Level 3 (L-3) action of the proposed mechanism. To incorporate this, there is need to confirm that a node is totally illegitimate before broadcasting its label "malicious" to all nodes. Therefore, the node that fails the CFG test is further examined using the elliptical curve cryptography technique using the Weierstrass elliptic function. Consider the coordinate points of the source and the next node N to be I and J, respectively; there is another point K which forms a straight line as illustrated in Figure 9.

The Weierstrass elliptic function is defined

$$\begin{aligned} y^2 &= x^3 + px + q \\ I + J &= K \quad \text{where } I \neq J,\ \forall I, J \in E, \end{aligned} \tag{8}$$

where (x_I, y_I) and (x_J, y_J) and (x_K, y_K) are the coordinates of the I, J, and K points forming an elliptic curve. Therefore, the coordinates (x_K, y_K) can be obtained from the following expressions:

$$\begin{aligned} x_K &= \beta^2 - x_I - x_J, \\ y_K &= \beta\left(x_I - x_K\right) - y_I, \end{aligned} \tag{9}$$

where $\beta = (y_J - y_I)/(x_J - x_I)$.

The commutative property of this function states that

$$I + J = J + K. \tag{10}$$

The working of this Level 3 test for publishing the node as malicious is given by Algorithm 2. The algorithm shows that the node estimates and sends $\mathrm{L3}_{\mathrm{REQ}}$ to the next node N.

```
(1)  Level3_ECC_Check()
(2)  {
(3)      S sends L3REQ to the next node N
(4)      Source S estimates FKEY ← I + J;
(5)      N replies with estimated RKEY ← J + K;
(6)      If (RKEY != FKEY){
(7)            Remove N from neighbor list
(8)            Broadcast N is "malicious" to all nodes
(9)            Return 1
(10)     } end if
(11)     Else {
(12)        Set false alarm high
(13)        Return 0
(14)     } end else
(15) } end
```

Algorithm 2

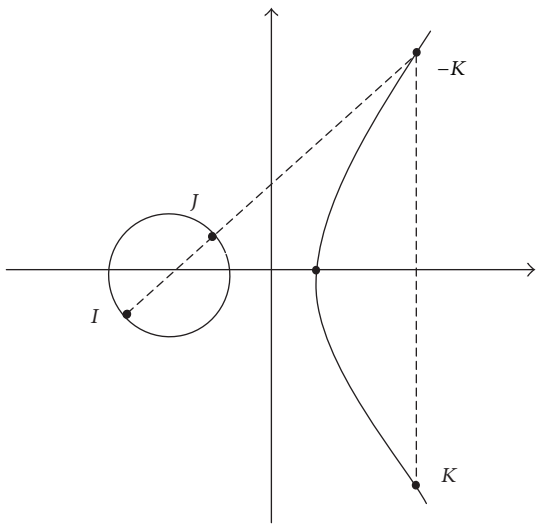

Figure 9: Elliptic Curve representing source and next node coordinates I and J.

Meanwhile the F_{KEY} is estimated using (11) at the source end. The next node replies to the $L3_{REQ}$ with R_{KEY} using (12):

$$F_{KEY} = I + J, \tag{11}$$

$$R_{KEY} = J + K. \tag{12}$$

The source node S compares its F_{KEY} with the R_{KEY} to conclude that the next node N is a malicious node. When F_{KEY} is not same as R_{KEY} then the node is published as malicious to all other nodes and the next nearest node is considered for communication. Algorithm 2 is a part of the main Algorithm 1.

5. Performance Metrics

Five metrics are assessed in the simulation analysis of the network. They are Packet Delivery Ratio, Packet Loss Ratio, Throughput, Delay, and Detection Rate.

5.1. Packet Delivery Rate. Packet Delivery Rate (PDR) is the ratio of the total number of packets successfully delivered to the total packets sent. It is obtained from (13) below, where n represents the total number of nodes in the networks:

$$\text{PDR} = \frac{\sum_0^n PktsDelivered}{\text{Time}}. \tag{13}$$

Here *PktsDelivered* is the number of packets received by the destination and *PktsSent* is the number of packets sent by the source.

5.2. Packet Loss Rate. Packet Loss Rate (PLR) is the ratio of the packets lost to the total packets sent, estimated by

$$\text{PLR} = \frac{\sum_0^n PktsLost}{\text{Time}} \quad \{0 \le \text{PLR} \le \infty\}. \tag{14}$$

5.3. Throughput. Throughput is defined as the rate at data is successfully transmitted for every packet sent, evaluated by

$$\text{Throughput} = \sum_0^n \left(\frac{PacketsReceived * 8}{\text{Delay in ms}} \right) \text{kbps} \quad \{0 \le \text{Throughput} \le \infty\}. \tag{15}$$

5.4. Delay. Delay is defined as the time difference between the current packets received and the previous packet received, evaluate by (16) below, where n is the number of nodes:

$$\text{Delay} = \frac{\sum_0^n PktRecvd\ \text{Time} - PktSend\ \text{Time}}{n} \quad \{0 \le \text{PDR} \le \infty\}. \tag{16}$$

5.5. Detection Ratio. In this paper, we observe the detection ratio and false detection ratio of AODV and ACFG routing protocols. The detection ratio and false detection ratio are defined as (17) follows:

$$\text{DR} = \frac{D_{pn}}{T_{pn}} \quad \{0 \le \text{DR} \le 1\},$$
$$\text{FDR} = \frac{M_{pn}}{T_{nn}} \quad \{0 \le \text{FDR} \le 1\}, \tag{17}$$

where D_{pn} is the number of precarious node detected by one or more normal nodes, T_{pn} is the total number of precarious nodes, M_{pn} is the number of normal nodes misidentified as the precarious node by one or more normal nodes, and T_{nn} is the total number of normal node.

6. Experimental Results and Discussion

The Network Simulator-2 is used to study the performance of our precarious node detection and secure data transmission in MANETs. We apply the IEEE 802.11. MAC with channel data rate 10 Mbps. Remaining parameters are available in Table 1.

Table 1: Simulation parameters.

Parameter	Value
Simulation area	1000 × 1000 m
Number of nodes	30
Channel	WirelessPhy
Channel data rate	10 Mbps
Radio propagation model	TwoRayGround
Antenna type	Omni Antenna
Traffic models	CBR/TCP
CBR interval	1.0 ms
Communication model	UDP
Mobility model	Random way point
Simulation time	100

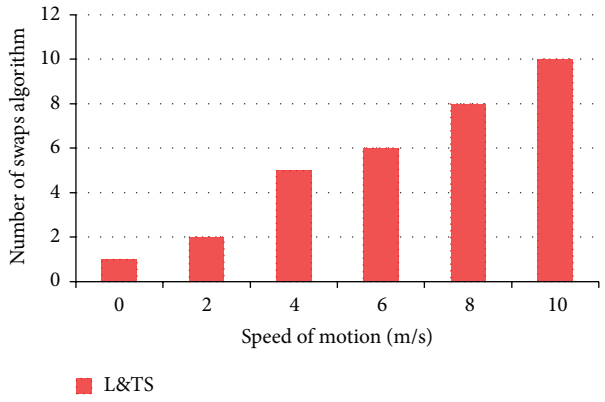

Figure 10: Effect of mobility in L&TS scheme.

6.1. Mobility Analysis. Mobility in MANETs is a hindrance for the implementation of many security schemes since it affects the QoS of the system. The security of L&TS scheme increases as the mobility increases. Figure 10 indicates mobility versus the number of swaps between the algorithms used. Greater the number of swaps, greater the security of the system. There is a tradeoff between QoS and security in this scheme.

6.2. Comparison of TMUR, L&TS, and ACFG with CBR Traffic Models. In order to validate the efficiency of the ACFG, we compare it with TMUR and L&TS protocol. The performance and metrics described in Section 5 are used here.

Figures 11 and 12 show the Packet Delivery Rate and Packet Loss Rate of the TMUR, L&TS, and ACFG mechanisms, respectively. These two metrics are proportional to each other and indicate the successful communication among the mobile nodes in any MANET. Therefore, it can be observed from the graphs that L&TS performs better than TMUR and ACFG performs better than both the mechanisms due to secure communication and the three-level checks performed over the nodes in the MANET.

Figure 13 shows the throughput obtained for the of TMUR, L&TS, and ACFG mechanisms. It can be observed that the maximum throughput obtained for ACFG is greater than the L&TS mechanism, which is in turn greater than the TMUR. Similarly, the delay observed in a MANET

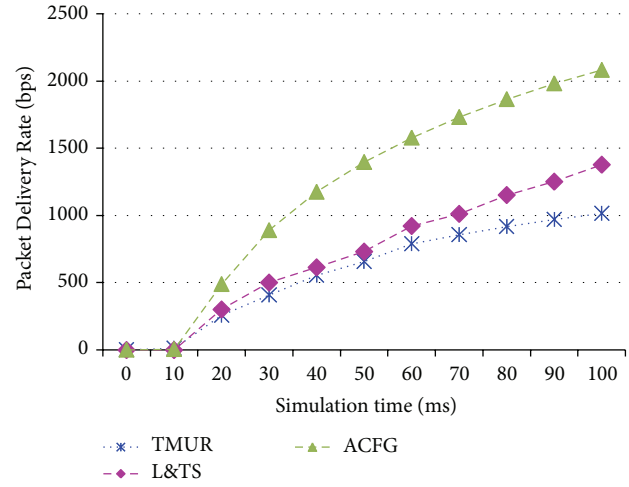

Figure 11: Packet Delivery Rate of TMUR, L&TS, and ACFG.

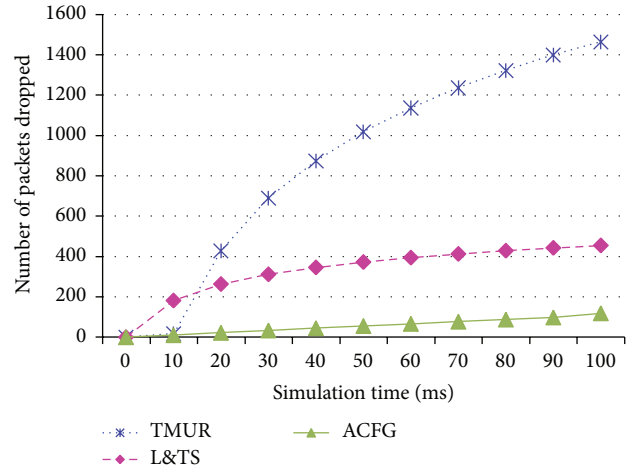

Figure 12: Packet Loss Rate of TMUR, L&TS, and ACFG.

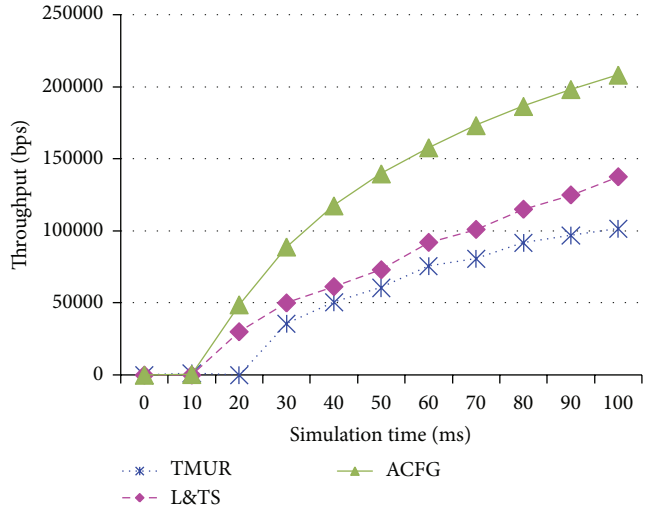

Figure 13: Throughput of TMUR, L&TS, and ACFG.

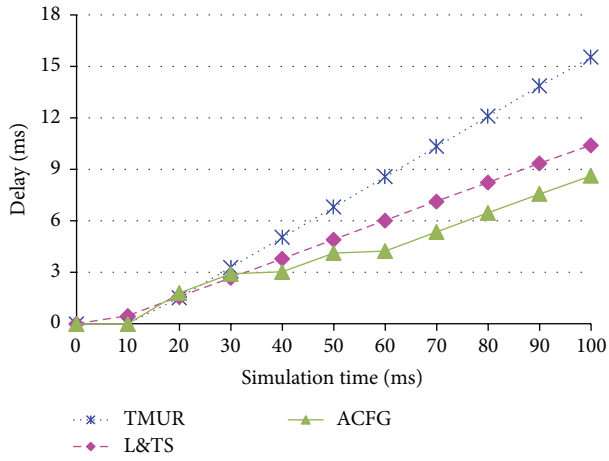

Figure 14: Delay of TMUR, L&TS, and ACFG.

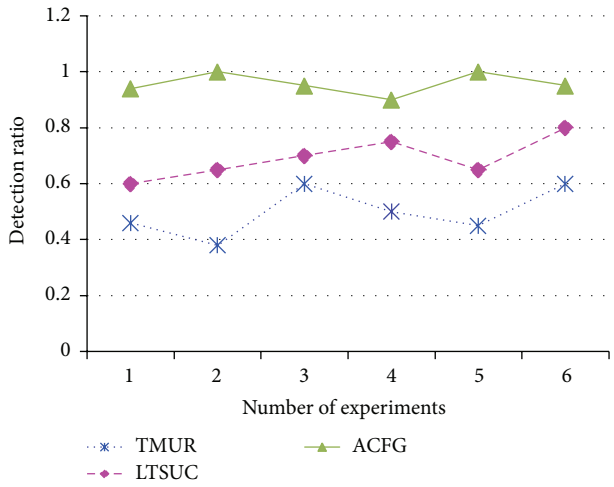

Figure 15: Detection ratio of TMUR, L&TS, and ACFG.

operated using the three protocols is also plotted in Figure 14. The ACFG mechanism shows the least delay compared to the L&TS that is also lower than the TMUR protocol. The malicious nodes present in the network obstruct the communication in the network and therefore the ACFG mechanism both avoids and detects the best performance among the three protocols.

The detection ratio of TMUR, L&TS, and ACFG mechanisms is plotted in Figure 15. After modeling a 20% of the nodes as attack nodes, the three methods are tested whether they are able to efficiently identify and detect the malicious nodes. It can be observed from the figure that the detection rate of ACFG is greater than both L&TS and ACFG mechanisms. Also the false positive ratio is plotted for the three comparing mechanisms in Figure 16 to observe that the ACFG mechanism has the lowest false positive ratio.

6.3. Comparison of Throughput in CBR and TCP Models. The operation of the ACFG mechanism using both Constant Bit Rate (CBR) and Variable Bit Rate (VBR) traffic models are validated. UDP does not contain acknowledge packet (ACK)

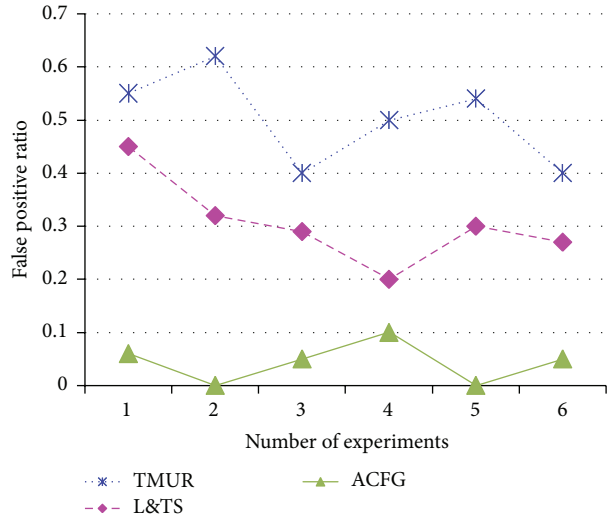

Figure 16: False positive ratio of TMUR, L&TS, and ACFG.

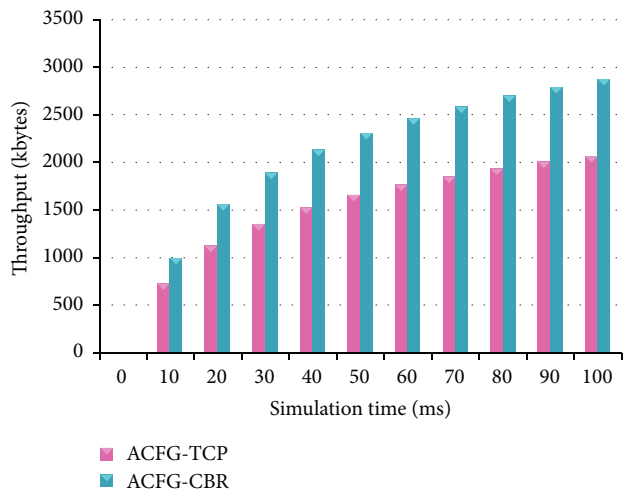

Figure 17: Throughput of ACFG with CBR and TCP models.

that permits the nonstop packet stream, as opposed to using TCP that acknowledges a set of packets calculated by using the TCP window size and Round Trip Time (RTT).

Figure 17 shows the throughput of ACFG with both CBR and TCP models. ACFG works better with CBR traffic model when compared with the TCP models. Figure 18 shows the throughput of the L&TS for CBR and TCP traffic models. The CBR generates slightly longer throughput than TCP. The CBR traffic model is better when compared to the TCP.

6.4. Comparison of Throughput against Node Mobility. In Figure 19, it can be observed that the TMUR suffers more from the speed of motion compared with the ACFG and L&TS. The security in TMUR does not vary under mobility because the mobility is increased when security algorithm is increased. Hence, the throughput does not change based on the mobility. However, ACFG obtains better throughput rate, compared to TMUR.

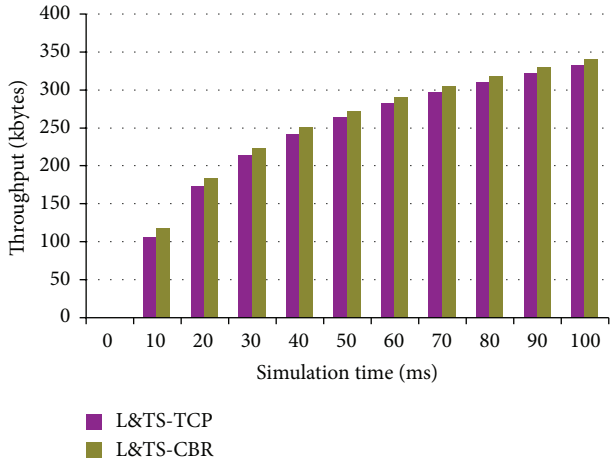

Figure 18: Throughput of L&TS with CBR and TCP models.

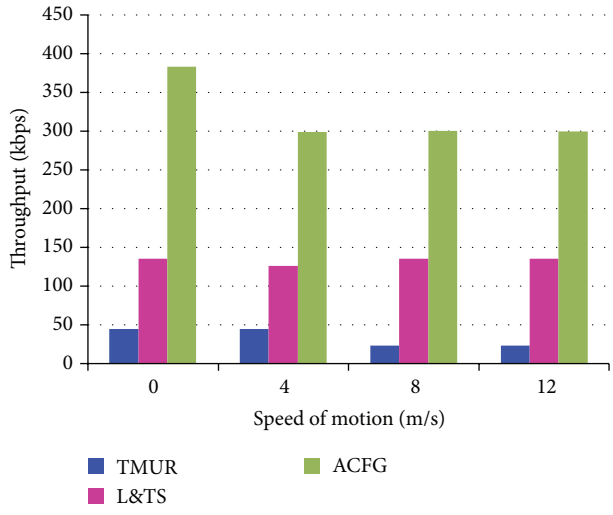

Figure 19: Throughput against node mobility.

6.5. Comparison of Throughput against Number of Nodes. According to analysis performed, the scalability of the proposed mechanisms is achieved by obtaining the throughput varying the number of nodes from 25 to 150 within an area of 1000 × 1000 m simulation field. From Figure 20, it has been observed that ACFG performs better than L&TS with average throughput crossing 3000 kbps.

A summary of the results shown in Figures 10–20 is tabulated in Table 2. The various parameters measured for TMUR, L&TS, and ACFG are tabulated to analyze the overall improvements.

The simulation results show that the dynamic estimation of the metrics improves throughput by 26% in L&TS when compared to the TMUR. ACFG achieves 33% and 51% throughput increase when compared to L&TS and TMUR mechanisms, respectively.

Table 2: Comparison of results.

Parameters	TMUR	L&TS	ACFG
Packet Delivery Rate (bps)	1015	1376	2083
Packet Loss Rate (packets)	1465	454	118
Throughput (bps)	101599	137604	208319
Delay (ms)	15.5	10.4	8.6
Average detection ratio	0.49	0.69	0.95
Average false positive ratio	0.50	0.30	0.04

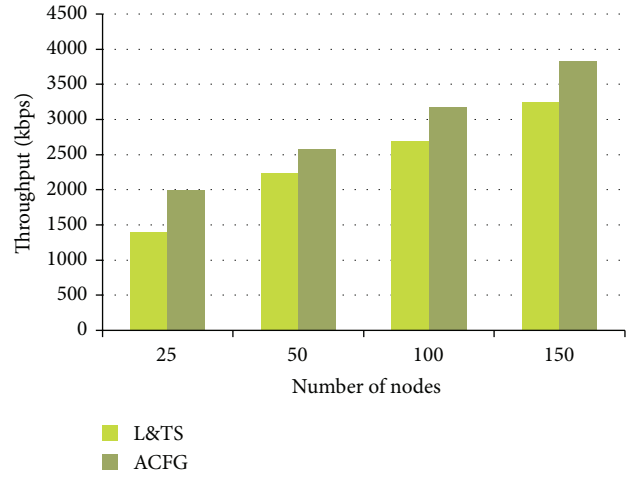

Figure 20: Throughput against number of nodes.

7. Conclusions

In this paper, we have proposed two new mechanisms for incorporating secure communication in MANETs. This paper contains two strategies: Location and Trust-based secure routing (L&TS) as well as Angle and CFG based precarious node detection (ACFG) with secure data transmission in MANETs. L&TS method uses various cryptography algorithms based on distance and includes trust based routing. ACFG method isolates the precarious node based on the Angle and Context Free Grammar and secures data transmission using the SHA-1 algorithm. The simulation results evaluate that both the ACFG and L&TS mechanisms offer improved throughput and reduced delay, more so the ACFG. In future works, we intend to investigate the precarious node detection in Cognitive Networks.

Conflict of Interests

The authors of this paper have no conflict of interests.

References

[1] B. Dahill, B. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," Tech. Rep. 01-37, University of Massachusetts, 2000.

[2] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS '02)*, San Antonio, Tex, USA, January 2002.

[3] Y. Zheng, Z. Peng, and V. Teemupekka, *Trust Evaluation Based Security Solution in Ad Hoc Networks*, Nokia Research Centre, 2006.

[4] K. C. Joshi and D. Pant, "Security of mobile Ad-hoc networks with five layer security architecture," Institute of Technical Teachers, 2010.

[5] M. Saleh and L. Dong, "Real-time scheduling with security enhancement for packet switched networks," *IEEE Transactions on Network and Service Management*, vol. 10, no. 3, pp. 271–285, 2013.

[6] 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.

[7] 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.

[8] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," *International Journal of Network Security*, vol. 9, no. 1, pp. 22–33, 2009.

[9] P. T. V. Bhuvaneswari, S. Karthikeyan, B. Jeeva, and M. A. Prasath, "An efficient mobility based localization in underwater sensor networks," in *Proceedings of the 4th International Conference on Computational Intelligence and Communication Networks*, pp. 90–94, IEEE, Mathura, India, November 2012.

[10] W. Heiko and J. Schiller, "Distance-based distributed multihop localization in mobile wireless sensor networks," in *8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze*, Hamburg, Germany, August 2009, http://page.mi.fu-berlin.de/eke/will09FGSN.pdf.

[11] A. Karma and J. Choudhary, "MPLI: a novel modified parametric location identification for AODV in MANET," *International Journal of Computer Applications*, vol. 100, no. 4, pp. 48–53, 2014.

[12] Z. Zhu, W. Guan, L. Liu, S. Li, S. Kong, and Y. Yan, "A multi-hop localization algorithm in underwater wireless sensor networks," in *Proceedings of the 6th International Conference on Wireless Communications and Signal Processing (WCSP '14)*, pp. 1–6, IEEE, Hefei, China, October 2014.

[13] J. Li, B. Halder, P. Stoica, and M. Viberg, "Computationally efficient angle estimation for signals with known waveforms," *IEEE Transactions on Signal Processing*, vol. 43, no. 9, pp. 2154–2163, 1995.

[14] C. Venkata and M. Singhal, "Angular routing protocol for mobile ad-hoc networks," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW '05)*, Columbus, Ohio, USA, June 2005.

[15] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Localization systems for wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 6–12, 2007.

[16] T.-F. Shih and H.-C. Yen, "Location-aware routing protocol with dynamic adaptation of request zone for mobile ad hoc networks," *Wireless Networks*, vol. 14, no. 3, pp. 321–333, 2008.

[17] P. K. Suri, M. K. Soni, and P. Tomar, "Framework for location based power aware routing in MANET," *IJCSI International Journal of Computer Science Issues*, vol. 8, no. 3, 2011.

[18] L. Cheng, C. Wu, Y. Zhang, H. Wu, M. Li, and C. Maple, "A survey of localization in wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 962523, 12 pages, 2012.

[19] R. M. Chamundeeswari and P. Sumathi, "Efficient detection of intrusion using inner and outer boundary models with transductive learning concept in mobile Adhoc network," *International Journal of Scientific & Engineering Research*, vol. 5, no. 6, 2014.

[20] A. Singh, D. Dagon, and A. L. M. Dos Santos, "Authentication protocols making use of context free grammar: guessing strings," Tech. Rep. GIT-CERCS-04-24, Georgia Institute of Technology, Atlanta, Ga, USA, 2004.

[21] S. C. Geyik and B. K. Szymanski, "Event recognition in sensor networks by means of grammatical inference," in *Proceedings of the 28th IEEE International Conference on Computer Communications (INFOCOM '09)*, pp. 900–908, IEEE, Rio de Janeiro, Brazil, April 2009.

[22] S. Jadhav and U. L. Kulkarni, "Natural language database interface with probabilistic context free grammar," *IJRIT: International Journal of Research in Information Technology*, vol. 2, no. 6, pp. 119–126, 2014.