INFORMATICA, 2020, Vol. 31, No. 1, 113–130


DOI: https://doi.org/10.15388/20-INFOR402

# Location Verification Technique for Cluster Based Geographical Routing in MANET

Balasubramanian MUTHUSENTHIL[1,2,*], Hyunsung KIM[3], V.B. Surya PRASATH[4,5,6,7]

[1] *Department of Computer Science and Engineering, Valliammai Engineering College, India*
[2] *Information Security Research Institute, Wookyoung Information Technology, Daegu, Republic of Korea*
[3] *Department of Cyber Security, Kyungil University, Republic of Korea*
[4] *Division of Biomedical Informatics, Cincinnati Children's Hospital Medical Center, OH 45229, USA*
[5] *Department of Pediatrics, University of Cincinnati College of Medicine, Cincinnati, OH, USA*
[6] *Department of Biomedical Informatics, College of Medicine, University of Cincinnati, OH 45267, USA*
[7] *Department of Electrical Engineering and Computer Science, University of Cincinnati, OH 45221, USA*
*e-mail: muthusenthilb.cse@valliammai.co.in, kim@kiu.ac.kr, prasatsa@uc.edu*

Received: March 2018; accepted: December 2019

**Abstract.** In mobile ad hoc network (MANET), routing has been the main issue because its high mobility and maintaining its routing structures are important requirements. Geographical routing mostly relies on real time location information, however, there exist lags in correctness of location information, and malicious nodes can cause troubles in accurate location tracking in the network. In order to ensure the correctness of location update information, in this paper, we propose a novel design based on a cluster based geographic routing (CBGR) formulation (Muthusenthil and Murugavalli, 2014), wherein we add a position verification technique based on a direct symmetry test (DST) to securely verify the location claims. We further introduce a new noise threshold parameter in the CBGR formulation to evaluate the correctness of location information based on a DST. Then a location based encryption scheme is employed to protect the estimated location against the eavesdropping attacks. With our simulation results, we show that the proposed location verification technique for CBGR (LVT-CBGR) network enhances the network security and performs better compared to other protocols in terms of performance metrics. The experimental outcomes illustrate the fact that our approach is well-geared to scale down the overall network expenditure.

**Key words:** mobile ad hoc network (MANET), location based routing, geographical routing, direct symmetry test, location attacks.

## 1. Introduction

An ad hoc network consists of a set of wireless mobile nodes to form a network cooperatively without any specific configuration or administration. A mobile ad hoc network

*Corresponding author.

(MANET) is a particular variant of a wireless network where the mobile hosts are connected wirelessly and form an unfixed infrastructure based temporary network. By forming a multi-hop radio network, the MANET nodes communicate to each other. The mobile node operates as an intermediate router. A number of hops are utilized to carry the data packets sent by a source node to reach a destination node. Due to this property, multi-hops are common in data communication and the final quality highly depends on node cooperation (Lin and Labiod, 2006). MANETs have been applied to various application areas including emergency search, rescue locations, military battlefields, deployment in disaster areas, etc. Such application areas typically warrant rapid deployments with active re-configuration a necessity. These networks can also be deployed locally, that is in a confined local area, such as conference halls, sports stadiums, small aircrafts, taxicabs, boats etc. One of the main characteristics of an ad hoc network is usually a lack of resources such as limited bandwidth and/or battery power constraints. Hence, routing in a MANET setting is challenging and requires further research (Zou and Chigan, 2009).

### 1.1. *Geographical Routing in MANETS*

In geographical routing mobile nodes in a network are able to ascertain their positions thanks to certain positioning systems such as a GPS, and a source can utilize some kind of location service to obtain the corresponding destinations. Intermediate nodes achieve forwarding decisions of packets using the knowledge of the immediate neighbour positions, and the source appends the destination's position in the packet header. In a default setting, the data packets are forwarded greedily through to the neighbour nodes thereby allowing the greatest geographical progression toward the destination. However, whenever such a neighbour does not exist, forward is used to recover the local gap perimeter. In this case, the packets travel across the planar local topology subgraph of the network by using the right-hand rule and progress until greedy forwarding can be restarted again. Although better than a global topology-based routing, imprecise knowledge of a local geographical topology, as well as destination positions, reduces the geographical routing performance. In current geographical routing protocols, each mobile node of the network periodically broadcasts a positional beacon to achieve a local geographical topology. However, in high dynamical scenarios, such proactive protocols create a lot of control overhead information even when there is no traffic through the system, as well as outdated results of the topology. Furthermore, reliance on one-hop forwarding of topological information in these geographical routing protocols leads to sub-optimal forwarding and blind forwarding in current systems (Xiang *et al.*, 2007). In general, geographical routing utilizes node locations to identify viable paths to the nodes. Furthermore, nodes not only know their own locations but also their one-hop neighbours. Since the system follows geographical routing, the destinations are explicitly described geographically (a region or a location), with each packet holding a small amount (O, 1) of routing information in the systems (Rathidevi and Kumaran, 2015).

### 1.2. *Location Verification Technique*

Malicious nodes can affect the forwarding decisions and a location verification technique (LVT) is utilized to check the accuracy of given node positions collected in the neighbour information table. This technique avoids possible errors in node positions in MANET and it is paramount to verify the node positions in the neighbour before choosing the nodes for forwarding packets in the network. Accuracies of the locations can be assured by position verification technique that utilizes the positioning systems. This technique finds the appropriate neighbours for forwarding the packets. A major bottleneck is the precision of such selected neighbour nodes and the identification of the proper ones. This is crucial in avoiding malicious node selection by hackers when selecting non-neighbours as true neighbours. Neighbourhood discovery process, also called the verification, ensures that the selected node is indeed in the right neighbourhood. Thus, after identifying the reliable and dependable nodes, verification technique is performed since the selected nodes are considered for validating other nodes (Papadimitratos *et al.*, 2008; Basha and Joshna, 2014). Position verification can still result in false positive and false negative rates since there are different types of attacks that can happen in the network. Due to limited message reception in typical wireless network settings, it is in general not always feasible to validate neighbourhood nodes with the neighbourhood discovery approach. Malicious hackers can manipulate the network nodes to disrupt communication between different nodes. Also, this can lead to the precise determination of true neighbourhood nodes surrounding the source node (Papadimitratos *et al.*, 2008). These misleading nodes, incorrectly identified as true neighbourhood nodes, lead to false position details at similar ranges (Basha and Joshna, 2014).

### 1.3. *Previous Work and Proposed Solution*

In prior research (Muthusenthil and Murugavalli, 2014), a protocol based on location supported cluster based geographical routing (CBGR) is proposed for intermittently connected MANET. In the previous CBGR protocol, degree difference based node value, node mobility, and residual energy are used to choose the head of the cluster. In this setup, there is a node with global positioning system (GPS) and a node with antenna. Moreover, the cluster consists of at least one G-node that selects the cluster head based on the information of remaining energy, speed and mobility of the nodes. In the ad hoc networks, due to the mobility of nodes the cluster maintenance is used to dynamically reorganize and reconfigure the overall cluster, and a store-carry forward model along with the geographical routing protocol is utilized. At the end, a location verification update technique is used to prevent location errors due to routing. By extending the work in Muthusenthil and Murugavalli (2014) and the CBGR protocol, our goal here is to design a position verification technique for the cluster based geographical routing in order to ensure the correctness of location update information. We therefore propose a location verification technique for cluster based geographical routing (LVT-CBGR) with the following features:

- It is modelled for hierarchical geographical ad hoc networks and without relying on the trusted infrastructure.

- It allows all nodes to perform all verification process autonomously.
- It is executed by any node at any point of time (i.e. reactive).
- It is independent, lightweight and robust as it generates low overhead traffic.

We organize the rest of the work as follows. In Section 2 previous location verification for geographical routing methods are presented. Section 3 shows position verification technique for the cluster based geographical routing in order to ensure the correctness of location update information. Finally, Section 4 discusses the experimental simulations of the proposed approach, and Section 5 provides the conclusions of our work.

## 2. Related Works

We briefly review related ad hoc network modelling and location verification approaches that are relevant to the work presented here. Liu *et al.* (2010) studied a node-to-node location verification method, wherein they make use of pairs of neighbourhood nodes for detection and target in the network, and determine the target and position of every pair by using one detect node and two globally active detective nodes. For location determination the distance is calculated based on these nodes. The location claim validation that lets the detecting node to clarify the location declaration of TN is supported by recognizing the compromised TN with the false location declaration and safeguarding the benign TN from overhearing when transmitting messages with the help of a new location based encryption technique and by not needing any kind of pre-shared secret keys.

Lo *et al.* (2013) have presented a geographical forwarding scheme for VANETs with location verification to determine the forwarding node in order to identify a proficient and steady node, in this case, a vehicle, so it can be used as a forwarding node in the network. After that, the calculation of link time, as well as the signal to noise ratio of the given signal, are used to affirm the chosen node is not only steady but also able to maintain longer persistent link time with the information providing nodes. To verify the location accuracy of surrounding nodes collected in the lookup table, a general verification technique is employed. Thanks to this location verifying technique, false nodes are found and can be removed immediately, and the vehicles that positively clear the verification test are selected as the successor forward node.

Fiore *et al.* (2013) proposed to identify and verify neighbourhood node positions in a MANET setting by using a special verifier node that determines and validates the positional information. In this approach, the special verifier aggregates the details of one-hop neighbourhood nodes and computes neighbourhood distances between nodes. Nodes then communicate with ascertained neighbourhood nodes using broadcast of POLL and REPLY messages. It then records the overall communication time between two nodes. To execute the time of flight based ranging, the verifier node broadcasts a REVEAL message and the neighbourhood nodes propagate the REPORT message to the verifier node which consists of identity and timing information. This helps in estimating the neighbourhood nodes and verifier distances between them. With these results obtained, each node is categorized into faulty, unverifiable, verifiable if sufficient node details are not available.

Shen and Zhao (2013) studied a new protocol for MANETs using an anonymous location based efficient routing terms, abbreviated as ALERT. In their approach, the network is split into zones using the protocol with a sender or a forwarder node. GPSR algorithm is utilized in these zones to move data toward the forwarder nodes for developing a reliable and smart path for intermediate relay nodes. In the next step, message propagation reaches the destination zone nodes without identification details. In this model, the source is kept anonymous and without details for security purposes of not revealing the source and destinations. In a similar approach, to handle privacy, El Defrawy and Tsudik (2011) proposed a system called privacy-friendly routing in suspicious MANETs (PRISM). It works based on the global group signature approach, and a tracking resistant method is utilized for location based on forwarding across the network. The source node broadcasts a RREQ message that has the group signature and a time stamp. This further contains an encrypted version of a session key. The destination node then examines the validity of time stamp from the source node, and if it is valid, it provides the response RREP upon receiving RREQ. This again is further encrypted with the session key as before. If it is not valid, then the RREQ is discarded. Upon obtaining the RREP message, the source node decrypts it with the session key. Note that here the destination node provides the location information, as well as validates the signature that is being sent. Finally, in the scenario where RREP is cached and executed priorly, the source node drops RREP message altogether.

Adnan *et al.* (2017) have presented a bound collection window for a sufficient collection time and verification cost for both attacker identification and isolation. Sheet *et al.* (2017) proposes two layered location information verification cum security technique based on transferable belief model. Rajakumar *et al.* (2017) proposed a method to search out the geographical position of unknown nodes with the help of anchor nodes in WSN using grey wolf optimization. Malandrino *et al.* (2014) suggested server based approach A-VIP for location verification uses a trusted server to verify location claims which reduces the applicability due to increasing demand of distributed approach. Various location verification schemes have been discussed in detail.

## 3. System Model

We describe our system model here and provide the details of our LVT based CBGR formulation along with metrics used to evaluate the overall system. We assume the evenly distributed nodes in the network with the network size of $A \times A$ and the number of nodes with $n = i + j$. The transmission range $r_i$ of the node $i$ varies from 5 to 10 m. Figure 1 shows the network configuration which consists of nodes *NG* – nodes with GPS, and *NA* – nodes with antennas. Furthermore, the network can be formed into clusters, and to save energy, the *NG* nodes may go to sleep or change to wake-up modes periodically. The *NA* nodes have enough capacity to send and receive signals to and from other nodes. These nodes also compute, from other nodes in the network, the received signal strength and the angle of arrival of the received signal information.

In the network studied here we consider all the other nodes as communication nodes that can be reached directly from a node under consideration. In order to achieve this, we have made the following assumptions in this work:

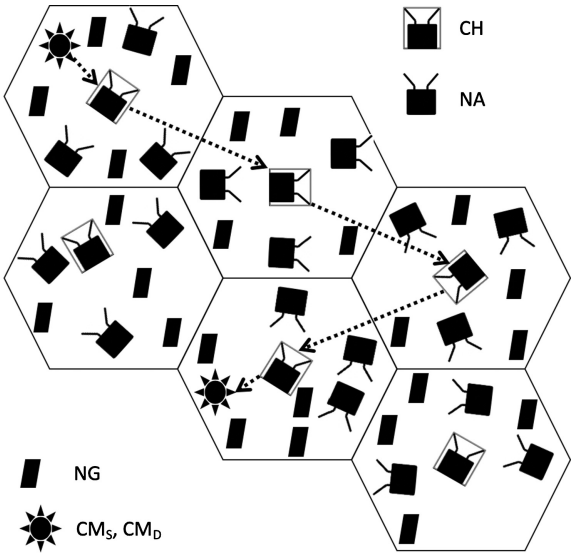


Fig. 1. Architecture setup of the proposed model.

1. Each node knows its own position thanks to GPS receivers and shares ir with other nodes with maximum tolerance and ranging error.
2. Node positions do not vary during message exchange which takes place in less than few ms.
3. Each node carries unique identity authenticated by location based encryption scheme.

### 3.1. *Overview of the Architecture*

In this work, we study a design with location verification technique for the cluster based geographical routing (LVT-CBGR) in MANET. In this technique, a direct symmetry test (DST) is used to securely verify the location claims. Then a location based encryption scheme is employed to protect the estimated location against the eavesdropping attacks. Note that our network architecture consists of the cluster head ($CH$) and the cluster member ($CM$) as the main entities.

**Cluster head ($CH_i$):** This is the coordinating node in each of the clusters. Here, we make an assumption that only *NA* node could be a candidate for the cluster head. Any *NA* node that has the maximum weight factor but a smaller mobility factor in a cluster could be selected as the cluster head.

**Cluster member ($CM_i$):** These nodes represent members of the network and perform some processing, gathering information and communicating with the cluster head in the network. Any *NA* or *NG* nodes which are attached to *CH* exclusively in each cluster could be member nodes.

We design the following transmission model based on the above main entities. This transmission occurs between a source node ($CM_S$) and a destination node ($CM_D$), and can be summarized as:

Table 1
Summary of notations and their representations used in this work.

| Notation | Representation of the symbol or symbol |
|---|---|
| $\Delta d_i$ | Degree difference |
| $ND_i$ | Node degree |
| $z$ | Size of the cluster |
| $m_i$ | Node mobility |
| $(u_1, v_1)$ and $(u_2, v_2)$ | Coordinates of the node $i$ |
| $E_i$ | Initial energy of a node |
| $E(t)_i$ | Energy consumed by the node |
| $n_{\text{tx}}$ and $n_{\text{rx}}$ | Number of data packets transmitted and received by the node after time $t$ |
| $\alpha$ and $\beta$ | Values in the open unit interval $(0, 1)$ |
| $E_{\text{res}}$ | Residual energy |
| $\mu_i$ | Weight factor for node $i$ |
| $x_1$, $x_2$ and $x_3$ | Weight values |
| $Q_i$ | Independent random variable |
| $N_i$ and $N_j$ | Neighbour nodes |
| $\|\|N_i - N_j\|\|$ | Euclidean distance between the nodes locations |
| $\epsilon(y)$ | Probability of a standard normal random variable |
| $S$ | Verifier |

1. If $CM_{\text{S}}$ is located within the transmission range of $CM_{\text{D}}$, $CM_{\text{S}}$ propagates the packet information to $CM_{\text{D}}$. This is done via the cluster head $CH_{\text{S}}$.
2. If $CM_{\text{D}}$ is not within the transmission range of $CM_{\text{S}}$, then the packet information is sent to the in the direction of $CM_{\text{D}}$ via the intermediate cluster heads.

### 3.2. *Metrics Utilized for Estimation in the Network*

We describe the main metrics utilized for network estimation and also further introduce a new noise threshold criteria that is not considered in the prior works (Muthusenthil and Murugavalli, 2017). This helps us to evaluate the correctness of location information based on the direct symmetry test (DST). Table 1 lists the parameters that are presented here.

**Degree difference** $(\Delta d_i)$**:** The degree difference metric $\Delta d_i$ is the difference among the total size of the cluster and node degree. This metric provides an estimate of the number of residual number of nodes that can be managed by each node in the network.

$$\Delta d_i = |ND_i - z|, \tag{1}$$

where $ND_i$ = node degree, and $z$ = size of the cluster (i.e. the number of nodes within the cluster).

**Node mobility** $(m_i)$**:** This metric node mobility is based on the coordinates of the nodes, and is given by

$$m_i = \frac{1}{T_2 - T_1}\sqrt{(u_2 - u_1)^2 + (v_2 - v_1)^2}, \tag{2}$$

where $(u_1, v_1)$ and $(u_2, v_2)$ are the coordinates of the node at time $T_2$ and $T_1$.

**Residual energy** ($E_{\text{res}}$)**:** The residual energy is computed based on the initial energy of a node $E_i$ and subtracting out the energy consumed by a node after a time period $t$. We let the energy consumed by a node ($E(t)$), and it is computed based on a formula that utilizes the number of data packets information transmitted and received:

$$E(t) = n_{\text{tx}} \times \alpha + n_{\text{rx}} \times \beta, \tag{3}$$

where $n_{\text{tx}}$ and $n_{\text{rx}}$ are the number of data packets transmitted and received by the node after time $t$, respectively. The parameters in the above formula $\alpha$ and $\beta$ are in the open unit interval of values (0, 1). Then the residual energy ($E_{\text{res}}$) for a node at time $t$ is computed by,

$$E_{\text{res}} = E_i - E(t). \tag{4}$$

**Noise threshold:** Let $Q_i$ be the independent random variable for the location estimation error. Let $\tau_i$ and $\psi_i^2$ be the mean and variance of $Q_i^2$. If the estimated location of $N_i$ is accurate, then probability distribution of $\tau^2$ for $\tau^2 \leqslant \tau_0^2$ corresponds to:

$$\lim_{n\to\infty} F\left[\tau^2 \leqslant \tau_0^2\right] = \varepsilon\left(\frac{n\tau_0^2 - \psi}{\delta}\right), \tag{5}$$

where $\psi = \sum_{i=1}^{n} \psi_i, \delta = \sqrt{\sum_{i=1}^{n} \delta_i^2}$ and $\varepsilon(y)$ is the probability of a standard normal random variable being less than $y$. As $\psi$ and $\delta$ are measured by ranging techniques, priority for the neighbour nodes $N_i$ and $N_j$ is estimated. Then the probability $\tau^2 \leqslant \tau_0^2$ for the benign node can be uniquely estimated using $\tau_0^2$. $\tau_0^2$ should be estimated satisfying the following condition:
The cumulative distribution $F[\tau^2 \leqslant \tau_0^2]$ should be closer to 100%. If a benign $N_i$ is cooperating well with $N_j$ in location estimation, then $\tau^2 < \tau_0^2$, else $\tau^2 > \tau_0^2$.

Note that $\tau_0^2$ should be set accurately due to following reasons: If it is set too small, then the accurate estimated location would be considered inaccurate; otherwise, the inaccurate estimation would be considered accurate.

Next, we recall the main steps in a general clustering approach in the following steps:

1. Initially at the deployment of nodes in the network, a broadcast message of *Hello* is sent to its neighbours with the specific format of the message. Note that the *Hello* message consists of the following five parameters, namely node ID, node location (obtained using GPS), node degree difference (1), node mobility (2), and the residual energy (4).
2. The neighbours list (NL) is maintained by each using the original *Hello* message along with their self node ID. Each node now estimates a node factor using the above parameter values and unitary weight values $x_1$, $x_2$ and $x_3$ with $x_1 + x_2 + x_3 = 1$,

$$\mu = (x_1 \times \Delta d_i) - (x_2 \times m_i) + (x_3 \times E_{\text{res}}). \tag{6}$$

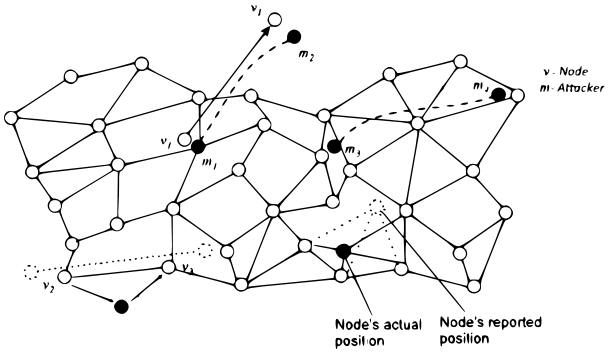


Fig. 2. Possible attacks on sensor nodes in a MANET. Here we show attacks that can tamper the location information of true nodes thereby altering the actual position of a node.

```
1: if m_i (node mobility) = NULL then
2:     Maximum node value, denoted by μ_max, can be obtained
3: end if
```

3. After estimating the node factor, each node then forwards to its one-hop neighbours $\mu_{\text{mes}}$ value.
4. The highest value $\mu_{\text{mes}}$ based node is then selected as the cluster head ($CH$). This selected node then transmits to its neighbourhood nodes a cluster head selection message ($CH$_Select), see Fig. 1. This message contains the information about the node that is selected as $CH$ along with neighbourhood table values.
5. As a final step, after receiving the sent message $CH$_Select from the cluster head $CH$, a join reply $J$_Rep is sent from neighbourhood nodes in $NL$ to $N_i$ for joining the cluster.

### 3.3. *Possible Attacks in a Location Based Routing Protocol*

We next describe the possible attacks on location based routing protocol considered in this work. Our experimental simulation results in Section 4.2 provide the testing of results for the attacks described here. Generally, the attackers can be broadly classified as malicious and compromised nodes. A malicious node is not involved in accessing the message content. A compromised node behaves maliciously and can access the message content as it is trusted by other nodes in the network. A compromised node can launch several attacks effectively without being detected even by the strong cryptographic techniques. Both the malicious and compromised nodes can launch various attacks against the location aided routing protocols. Some of the common attacks are discussed in this section. Figure 2 demonstrates the attacks on sensor nodes.

**Location information tampering attacks.** In this attack, the attackers are capable of modifying the content in location information packets. This attack includes impersonating other nodes and replaying packets with modified contents.

**Location falsifying attacks.** The adversaries intentionally announce a fake position to gain the network access and can create the network traffic in high level.

**Location information dropping attack.** In this attack, the adversaries intentionally drop some or all packets containing location information that are forwarded through it. It is known that MANET nodes act both as end hosts and routers. In this case, packet dropping attackers can destroy the entire functionality of the network with an increased number of attackers.

**Location table tampering attack.** In this attack, the content stored in the location information table is modified by the attacker. This type of attack can include the deletion, modification, and falsification of contents that are provided in the location information table in a node-wise manner.

**Clogging.** An attacker can initiate the neighbour position verification protocol several times over a short interval, and get the same challenge and reply message repeatedly from other nodes to congest or clog the communication medium. This adversarial action causes severe damage as the challenge messages are larger in size.

**Spoofing attack.** The adversaries can spoof the packets that contain the location information.

**Jamming attack.** The jamming adversaries block radio transmissions in a specified geographical region. Hence, the functioning of geographical routing protocol has to be prevented from using that area.

### 3.4. *Verification of Location Claims*

In order to verify the location claims in the MANET, here we propose to use the direct symmetry test (DST) to securely verify the location claims of cluster members $CM$. In the DST, each $CM$ of the cluster evaluates the communication neighbours with direct links. This means checking if the time of flight (ToF) distances are consistent with (i) one another, (ii) the location information propagated by the neighbourhood nodes, and (iii) a transmission range $U$. More specifically,

1. It not only verifies the distances $N_i$ and $N_j$ obtained from transmission range, but also checks whether these distances do not differ by more than two times the ranging error along with a tolerance value.
2. It further checks for the consistency of the advertised neighbourhood node location information within a prescribed error margin level.
3. Finally, a sanity check whether $\mu_{CHN_i}$ is not greater than $U$.

We utilize the DST to securely verify the location claims of the user and a similar usage was done by Fiore *et al.* (2013). Let $N_i$ and $N_j$ be the two neighbour nodes within the cluster respectively, $\|N_i - N_j\|$ be the Euclidean distance between the node locations, $\alpha$ be the tolerance value of the node mobility, $\beta$ be the ranging error, and $\lambda$ be the position error. Initially, in the DST based test, $CH_i$ performs the following:

1. It verifies the direct links with its neighbours within the transmission range, i.e. if

$$|\mu_{CHN_i} - \mu_{N_iCH_i}| > 2\alpha + \beta.$$

The above statement reveals that $CH_i$ verifies whether the distance $\mu_{CHN_i}$ and $\mu_{N_iCH_i}$ measured through ranging is not more than twice the $\alpha$ value along with the $\beta$ value.

2. It verifies whether, within an error margin, the position established by the neighbour is consistent with the obtained distances, i.e. $\|CH_i - N_i\| > 2\lambda + \beta$.
3. It verifies whether $\mu_{CHN_i}$ is not greater than $U$, i.e. $\mu_{CHN_i} > U$.

```
if |μ_CHN_i − μ_N_iCH_i| > 2α + β then
    if ‖CH_i − N_i‖ > 2λ + β then
        if μ_CHN_i > U then
            It is concluded that DST is verified
        end if
    end if
end if
```

Note that $U$ refers to the maximum nominal transmission range, and it is greater than the distance at which two nodes can communicate. If there is a mismatch in the above three verification rules, then the neighbour node is marked as defective.

### 3.5. *Location Based Encryption Scheme*

Once the location of the node is estimated, it is required to protect the location claim from eavesdropping and verify the consistency between the location $Q$ and location claims $QC$. Let $\tau_0^2$ be the noise threshold for the given estimated location, then we use the following scheme to check and protect.

1. $CH_i$ estimates the $\mu_{CHN_i}$ of $N_i$ through ranging in Section 3.2.
2. For $\mu_{CHN_i}$

```
if τ² > τ₀² then
    It is concluded that the location is incorrect
    N_i is marked as malicious.
end if
```

The noise threshold $\tau_0^2$ is estimated in Section 3.2.

3. $N_j$ generates the $n \times n$ key matrix $M$ and transmits it to $N_i$ along with a group of geographical indexes $(X, Y)$, where $M$ holds the $n \times n$ key for encryption and the indexes are used for mapping a key to a pair of geographical coordinates.
4. $N_i$ finds a key $m_{g,h}$ based on its location claim $QC$ and encrypts $QC$ using this key i.e. $K = Em_{g,h}(QC)$.
5. $N_i$ transmits the encrypted location $K$ to $N_j$.
6. Once $N_i$ receives $K$, it decrypts the locations by tracking the key using the estimated location $Q$.

We illustrate this scheme with the following example.

Table 2
Simulation parameters used in network simulator NS-2 for testing the performance of our proposed location verification technique for cluster based geographical routing (LVT-CBGR).

| | |
|---|---|
| Number of nodes | 20 to 100 |
| Area size | 1200 × 1200 m |
| MAC protocol | 802.11p |
| MAC data rate | 5 Mbps |
| Simulation time | 600 s |
| Traffic source | CBR with 6 packets/s |
| Channel type | Wireless |
| Packet Size | 512 bytes |
| Packet type | UDP |
| Number of attackers | 10 to 30 |
| Tranmission range | 300 m |
| Transmit power | 0.375 W |
| Receiving power | 0.375 W |
| Idle power | 0.1 W |
| Initial energy | 7 J |
| Antenna | Omni |

EXAMPLE 1. Consider the following scenario: $\tau = 0$ and $Q = QC$.

- Here, $Q$ and $QC$ would be mapped to same key $m_{g,h}$.
- If $\tau \neq 0$, then $Q$ may get deviated from $QC$. Here, the key $m_{g',h'}$ found by $Q$ will be different from $m_{g,h}$.
- Hence, a local search is performed around $m_{g',h'}$ and search range is determined based on $\tau_0^2$.
- In particular, $N_j$ selects a $\left(\frac{2\tau_0}{QC+1}\right) \times \left(\frac{2\tau_0}{QC+1}\right)$ sub-matrix and $M'$ with $m_{g',h'}$ as center.
- If $N_0$, a benign node, helps $N_j$ in estimating $Q$ and offers an honest $QC$, $m_{g,h}$ should be within $M'$. That is, $(Q - QC) < \tau_0$.
- Then $N_j$ estimates through a local search.
- However, if $N_j$ cannot find the correct key for decryption, then $N_i$ is considered to be malicious node.

## 4. Performance Analysis

### 4.1. *Experimental Setup and Performance Metrics*

We used the network simulator NS-2 (Fall and Varadhan, 2007) to test the performance of our proposed location verification technique for cluster based geographical routing (LVT-CBGR) and to perform comparisons. Table 2 summarizes the simulation parameters used. Our simulation environment consists of the following key components:

- Routing, namely geographical routing (Muthusenthil and Murugavalli, 2017);
- Node mobility and data traffic;
- Attacker model;
- DST based verification system.

We used these components in the following specific settings for illustrative purposes.

**Geographical routing** For our study, we utilized a greedy routing. This approach chooses the neighbour nearest to the destination as next hop for packets. In case of failure due to the unavailability of next hop, right hand thumb govern is applied, i.e. packets are put away locally until either an appropriate neighbour is reachable or until the packet drops due to overflow.

**Node mobility and data traffic scenario.** The simulation mainly considered two parameters: data traffic and node mobility. As data traffic, 100 messages are transmitted from a $CM_S$ source node to a $CM_D$ destination node. These messages are created between simulation time $t = 0$ s and $t = 30$ s.

**Attacker model.** Attacker nodes are implemented based on these models.

- Whenever an attacker node uses random position field in its group and sends a beacon message to announce its present position instead of its actual position.
- Whenever a malicious node gets a data packet, falsifying the position of its own and rerouting packets, sometimes even being dropped to disconnect routes.

**Verification system.** This based on the DST for all the nodes in the network.

The performance of LVT-CBGR is compared with a secure location verification protocol (SLVP) studied in Lo *et al.* (2013). To evaluate the performance of the models we utilized the following metrics of quality used widely in MANET settings.

**Average end-to-end delay.** The end-to-end-delay is averaged over all surviving data packets from sources to the destinations.

**Average packet delivery ratio.** It is the ratio of the number of packets received successfully and the total number of packets transmitted.

**Overhead.** It is the number of packets dropped during the data transmission.

**Location error.** It is the adversary nodes during one-hop transmission in packet forwarding.

**Throughput.** It is the number of packets successfully delivered from source to destination per second with attacker's false location claims.

### 4.2. *Results and Discussion*

We next report the performance of the above metrics based on our simulation results with respect to varying the number of nodes as well as the number of attackers.

**Varying the number of nodes.** We varied the total number nodes in the network from 20 to 100.

Figure 3 shows the performance evaluation and comparison of the approach and the SLVP method with respect to the end-to-end delay. As the number of nodes goes up, the end-to-end delay is increased, which shows that the end-to-end delay of the proposed LVT-CBGR approach is smaller than that of the SLVP approach. It is established that the resilience of our LVT-CBGR method is around 66% smaller than the SLVP.

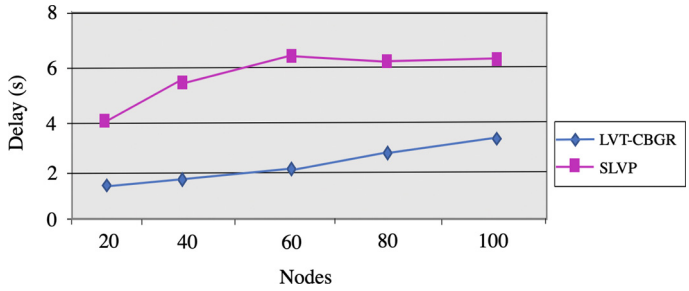


Fig. 3. Node vs Delay (s). Comparison of our LVT-CBGR and SLVP performance in terms of end-to-end delay as the number of nodes increases indicating that the proposed network obtains lowest delay (s).

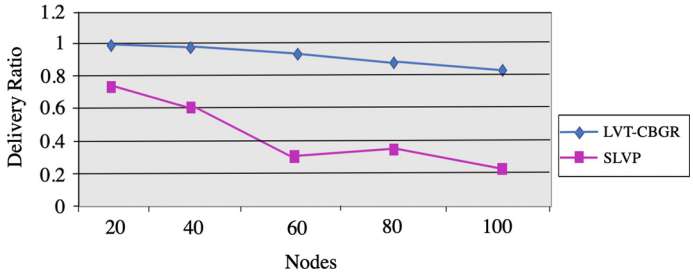


Fig. 4. Node vs Packet Delivery Ratio. Comparison of our LVT-CBGR and SLVP performance in terms of packet delivery ratio as the number of nodes increases shows that our proposed network obtains higher delivery ratios.

Figure 4 illustrates the packet delivery ratio when there is an increase in the number of nodes. It is clear that our LVT-CBGR technique ushers in superior delivery ratio as against the SLVP approach. At the outset, when the rate is 20, the packet delivery ratio is 30% larger than the SLVP approach. But the packet delivery ratio is reduced as and when the rate is stepped up, which also illustrates that the packet delivery ratio and the rate are inversely proportional to each other. But in all scenarios, our novel LVT-CBGR method yields superlative delivery ratio than the SLVP technique.

Figure 5 effectively displays the packet drop ratio for the LVT-CBGR and the SLVP approach. In the case of the proposed technique, the packet drop is smaller than that of the modern approach by around a high 70%.

**Based on the number of attackers,** we varied the total number of attackers from 10 to 30.

Figure 6 illustrates the performance evaluation and comparison of the approach and the SLVP method with respect to the packet delivery ratio. As the number of attackers goes up, the packet delivery ratio is reduced, which shows that the attackers are capable of adversely affecting the efficiency in performance of the method. Still, the packet delivery ratio of the novel approach is larger than the modern approach. It is established that the resilience of our LVT-CBGR method is around 34% greater than the SLVP approach.

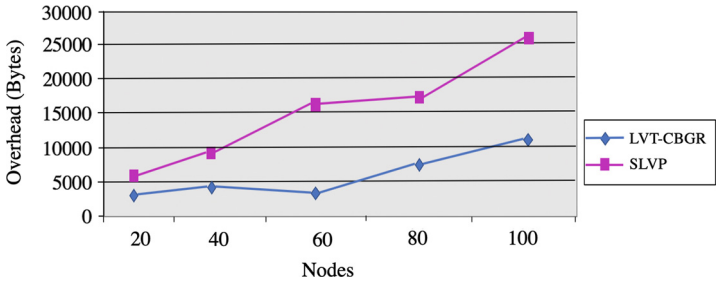


Fig. 5. Node vs Packet Drop Ratio. Comparison of our LVT-CBGR and SLVP performance in terms of packet drop ratio (bytes) as the number of nodes increases. Our LVT-CBGR obtains a smaller packet drop even when the nodes increase to 100.

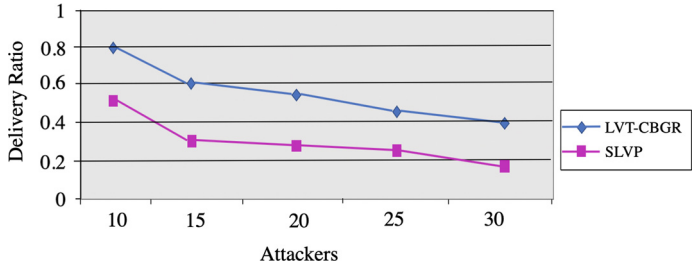


Fig. 6. Attackers vs Packet Delivery Ratio. Comparison of our LVT-CBGR and SLVP performance in terms of packet delivery ratio as the number of attackers increases shows that our approach is more resilient to attacks.

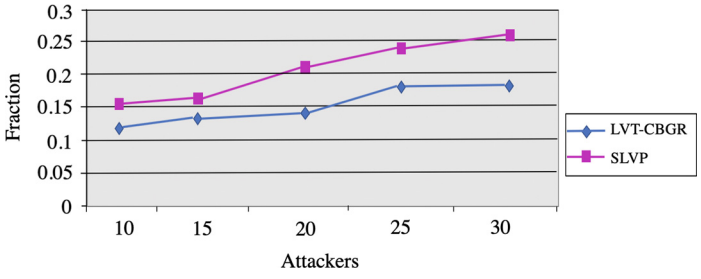


Fig. 7. Attackers vs Compromised Communication. Comparison of our LVT-CBGR and SLVP performance in terms of communication fraction compromised as the number of attachers increases. Our LVT-CBGR compromises less communication as the number of attackers increase to 30.

Figure 7 shows the performance evaluation and comparison of the approach and SLVP method with respect to compromised communication. As the number of attackers goes up, the compromised communication is increased, which shows that the attackers are capable of adversely affecting the efficiency in performance of the method. Still, the compromised communication of the approach is smaller than the SLVP approach. On analysis, it is established that the resilience of our LVT-CBGR method is around 28% smaller than the SLVP approach.

## 5. Conclusion

In this paper, we have proposed to design a location verification technique for the cluster based geographical routing (LVT-CBGR) in mobile ad hoc networks (MANETs). In this technique, a direct symmetry test (DST) is used to securely verify the location claims. Then a location based encryption schema is employed to protect the estimated location against the eavesdropping attacks. By introducing a new noise threshold parameter in the CBGR formulation, the consistency between the location and location claims are verified effectively. With experimental simulations, we obtained good results with varying number of nodes, in particular our results on increasing the nodes against delay(s) showed that the LVT-CBGR obtained low delay times. Moreover, when compared to a related approach, the LVT-CBGR obtained increased packet delivery ratios of 30% higher, and packet drop ratio of less than 70%, indicating superior performance in information communication across. Further experimental results on security against varying number of attacks showed that our LVT-CBGR is resilient even when the number of attackers was the highest, as vindicated by a delivery ratio higher by 34%, and 28% less compromised communication.

**Acknowledgements.** The authors sincerely thank the reviewers for their comments that helped revise our manuscript and improve the overall content and presentation of the work.

## Funding

This work was partially supported by the National Research Foundation of Korea Grand funded by the Korean Government (MEST) (NRF-2010-0021575) and by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

## References

Adnan, A.I., Hanapi, Z.M., Othman, M., Zukarnain, Z.A. (2017). A secure region-based geographic routing protocol (SRBGR) for wireless sensor networks. *PloS One*, 12(1), 170.

Basha, S.A., Joshna, G.P. (2014). Locating and verifying of neighbour positions in MANETs. *International Journal of Computer and Electronics Research*, 3(4), 220–222.

El Defrawy, K., Tsudik, G. (2011). Privacy-preserving location-based on-demand routing in MANETs. *IEEE Journal on Selected Areas in Communications*, 29(10), 1926–1934.

Fall, K., Varadhan, K. (2007). The network simulator (ns-2). http://www.isi.edu/nsnam/ns. Retrieved 05 July 2019

Fiore, M., Casetti, C.E., Chiasserini, C.F., Papadimitratos, P. (2013). Discovery and verification of neighbor positions in mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 12(2), 289–303.

Lin, H., Labiod, H. (2006). INGEO: indoor geographic routing protocol for MANETs. In: *Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking*.

Liu, D., Lee, M.C., Wu, D. (2010). A node-to-node location verification method. *IEEE Transactions on Industrial Electronics*, 57(5), 1526–1537.

Lo, C.C., Chen, S.C., Kuo, Y.H. (2013). Geographical forwarding scheme with location verification for vehicular ad hoc networks. In: *21st International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–5.

Malandrino, F., Borgiattino, C., Casetti, C. (2014). Verification and inference of positions in vehicular networks through anonymous beaconing. *IEEE Transaction on Mobile Computing*, 10, 2415–2428.

Muthusenthil, B., Murugavalli, S. (2014). Location aided cluster based geographical routing protocol for intermittently connected MANET. *International Review on Computers and Software*, 9(1), 1–9.

Muthusenthil, B., Murugavalli, S. (2017). Privacy preservation and protection for cluster based geographic routing protocol in MANET. *Wireless Networks*, 23(1), 79–87.

Papadimitratos, P., Poturalski, M., Schaller, P., Lafourcade, P., Basin, D., Capkun, S., Hubaux, J.P. (2008). Secure neighborhood discovery a fundamental element for mobile ad hoc networking. *IEEE Communications Magazine*, 46(2).

Rajakumar, R., Amudhavel, J., Dhavachelvan, P., Vengattaraman, T. (2017). GWO-LPWSN: grey wolf optimization algorithm for node localization problem in wireless sensor network. *Journal of Computer Networks and Communications*.

Rathidevi, E., Kumaran, N.S. (2015). Geographical routing in MANET using flexible combination of push and pull algorithm. *International Journal of Science and Research*, 2(3), 44–47.

Sheet, D.K., Kaiwartya, O., Abdullah, A.H., Cao, Y., Hassan, A.N., Kumar, S. (2017). Location information verification using transferable belief model for geographic routing in vehicular ad hoc networks. *IET Intelligent Transport Systems*, 11(2), 53–60.

Shen, H., Zhao, L. (2013). ALERT: an anonymous location-based efficient routing protocol in MANETs. *IEEE Transactions on Mobile Computing*, 12(6), 1079–1093.

Xiang, X., Zhou, Z., Wang, X. (2007). Self-adaptive on demand geographic routing protocols for mobile ad-hoc networks. In: *26th IEEE International Conference on Computer Communications*, pp. 2296–2300.

Zou, C., Chigan, C. (2009). An anonymous on-demand source routing in MANETs. *Security and Communication Networks*, 2(6), 476–491.

**B. Muthusenthil** received the bachelor's degree in electronics communication engineering from Madras University in 1996, master's degree from Satyabama University in 2007, doctorate from Anna University, Chennai, India, in 2016. Currently, he is a research scientist in Wookyoung Information Technology, Daegu, South Korea, and and associate professor at Valliammai Engineering College, Chennai. His interests are mobile ad-hoc networks, network security, video security, network attacks, privacy preservation, trust evaluation and cloud computing. He is affiliated with scientific publications and has served as an invited reviewer for many journals. Besides, he is also involved in NGOs, student associations, and managing of non-profit foundations.

**H. Kim** received his MSc and PhD degrees in computer engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2011 with the Department of Computer Engineering, Kyungil University. Currently, he is a professor at the Department of Cyber Security, Kyungil University. His current research interests are cryptography, VLSI, security protocols, network security and ubiquitous computing security.

**V.B.S. Prasath** is a mathematician with expertise in the application areas of image processing, computer vision, machine learning and data science. He received his PhD in mathematics from the Indian Institute of Technology Madras, India, in 2009. He has been a postdoctoral fellow at the Department of Mathematics, University of Coimbra, Portugal, for two years, from 2010 to 2011. From 2012 to 2015 he was a postdoctoral fellow at the Computational Imaging and VisAnalysis (CIVA) Lab, University of Missouri, USA, and from 2016 to 2017 he was an assistant research professor at the same institution. He is currently an assistant professor at the Division of Biomedical Informatics, Cincinnati Children's Hospital Medical Center, and at the Departments of Biomedical Informatics, Electrical Engineering and Computer Science, University of Cincinnati, from 2018. He had summer fellowships/visits at Kitware Inc. NY, USA, The Fields Institute, Canada, and IPAM, University of California Los Angeles (UCLA), USA. His main research interests include nonlinear PDEs, regularization methods, inverse and ill-posed problems, variational, PDE based image processing, and computer vision with applications in remote sensing, biomedical imaging domains. His current research focuses are data science, bioimage informatics with machine learning techniques based image processing, and computer vision with applications in remote sensing, bio-medical imaging, and biometrics domains.