Vulnerabilities of Internet Access Mechanisms from Mobile Ad Hoc Networks

Gautam Das  
Computer Science and Engineering  
Indian Institute of Technology, Guwahati  
Guwahati, India 781039  
gautam@iitg.ernet.in

M. Fazio, M. Villari, and A. Puliafito  
Università di Messina  
Dipartimento di Matematica  
Contrada di Dio, S. Agata, 98166 Messina, Italy.  
apulia{mfazio, mvillari}@ingegneria.unime.it

Abstract

Gateway node provides connectivity to the nodes inside MANET. Based upon the route to gateway node found during discovery phase; source node relies on intermediate nodes to forward packets to the gateway node. We have identified a vulnerability of the gateway discovery phase where adversaries can forcibly introduce routes having wormholes exploiting the routing race conditions. We have termed such routes having wormholes as the pseudo routes. The pseudo route attack is a more generalized form of the wormhole attack where wormhole start and end points can be any two nodes in the route and even multiple wormholes can be present in the same route. We have proposed an end-to-end approach using localization information to detect and prevent pseudo route attacks. Simulation results are presented to show the impact of pseudo route attack under various scenarios as well as for performance of the proposed protocol. We found that attack impact is more when the gateway is at the corner of the network.

1 Introduction

Applications of MANET have been envisioned mainly for the crisis solutions (e.g., in the battlefields or in the rescue operations) as well as civilian applications, most of which require the Internet connectivity. It involves a gateway discovery phase; which is performed either in an on-demand manner [9] or in a proactive manner [13]. In this work, we introduce pseudo route attack which a node can face during the gateway discovery phase. In this attack, an attacking node tunnels gateway discovery messages received from its neighbors during gateway discovery in one part of the network over a low-latency link and rebroadcast them in a different part; forcibly introducing routes better in terms of delay and hop count (called as pseudo route). The tunneling is achieved through the wormholes established by the attacking nodes.

The pseudo route takes the advantage of routing race conditions where wormholes introduce lesser hop routes (usually better routes in terms of delay and number of hops) and wins over other routes. Pseudo route attack involves two or more adversaries colluding to understate their distances from each other by relaying packets along an out-of-bound channel (defined by the wormhole start point and the end point) available only to the attackers. Consequently, pseudo route would be established reducing the hop count between the source node and the gateway node. The pseudo route attack is a severe threat against packet routing to the gateway.

The protocol design to mitigate the affect of the pseudo route attack is motivated by the philosophy of prevention is better than cure. In a scenario where nodes are mobile and routes to gateways are varying, the approach of detecting vulnerabilities after packet transmission through performance measurement such as throughput and then bad nodes reputation exchange causing such packet drop is not acceptable. This introduces extra overhead. The proposed scheme detects pseudo routes during gateway discovery itself rather than after routing to gateway and then measuring routing performance metrics. Due to this attack, a gateway node may respond positively to gateway discovery messages but then fail to forward the actual packets, intermediate nodes forming the wormholes may willingly drop the traffic through it. Fig. 1 shows an example of a pseudo route attack.

![Figure 1. Two attacking nodes form a wormhole. When they receive gateway discovery packets from nodes within its transmission boundary, they tunnel them through wormhole. This leads to the introduction of better routes (pseudo routes).](image)

Previous approaches for mitigating the impact of routing misbehavior[1, 2, 3, 7] require the nodes in the network to exchange reputation information about other nodes. Unlike existing protocols, this work considers the issue when a group of adversaries in the network jointly launch an attack and adopt the approach of prevention rather than detecting after it has occurred. Making a decision about whether to believe a node or not is a major issue and has high management cost. Such task could be performed offline or could be bootstrapped during network operation. In the former case, the network requires a priori
trust relationship that may not be practical in MANET. In the latter case, bootstrapping trust relationships in ad hoc networks involves significant complexity and risk. It is not reasonable for a dynamic and short-lived network.

1.1 Our contributions

This work is one of the first works that considers the vulnerabilities of the Internet access mechanisms from MANET. We have identified pseudo route attack and proposed a scheme to detect it before actual data transfer occurs. This eliminates most trust management complexity, albeit at a cost of less information with which to make decision about node behavior. We focus on detecting this misbehavior with only direct observations. We address the attack using a simple, lightweight approach that results in reasonable performance. To the best of our knowledge, this attack is the first generalized version of the wormhole attack. In this attack, impact of wormhole is considered for flooding based mechanism (i.e., the gateway discovery mechanism). In this form, colluding pair of nodes can be any two nodes in the route causing wormhole. Besides, pseudo route can even have multiple wormholes.

We present countermeasures at various levels starting from secure neighbor maintenance, through a simple structure called *Neighbor Table* (NT) to complete route analysis. The proposed scheme aims at maintaining the overall packet throughput during the Internet access in the face of node misbehavior at the routing layer. We concentrate our efforts at the routing layer and do not attempt to address attacks at lower layers.

The rest of the article is organized as follows. Section 2 describes recent work related to this area and few tradeoffs. A discussion on pseudo route attack and different geometric types are presented in Section 3. The Section 3.2 presents protocol to detect and prevent pseudo route attack. Section 4 presents the simulation results showing the impact of the pseudo route attack and performance of the protocol. Section 5 concludes the paper.

2 Related Work

Recently, security problems in MANET have received considerable attention by researchers. Different levels of trade-offs exist due to resource limitations of devices. Regarding misbehavior of nodes in the network, one of the protocols named CONFIDANT [1] detects misleading nodes by means of observation and more aggressively informs other nodes of misbehavior through reports sent around the network. Each node in the network hosts a monitor for observations, reputation records for first-hand and trusted second-hand reports, trust records to control the trust assigned to receive warnings, and a path manager used by nodes to adapt their behavior according to reputation information.

Wormhole attacks were independently discovered by three different works [11], [8] [5]. The work [14] reconstructs the layout of the sensors using multi-dimensional scaling to deal with wormholes and detects it by visualizing the anomalies introduced by the wormholes in the network layout. Packet leash [5] is another solution to deal with wormhole attacks. The leash is the information added into a packet to restrict its transmission distance. Recent work [4] leverages the benefits from directional antennae to defend against wormhole attacks.

3 Taming pseudo route attack

A bidirected graph \( G = (V,E) \) represents the network. Number of hops determined by gateway discovery phase is \( h(u,v) \). Here, \( u \) is the gateway node and \( v \) is the source node. This work assumes that \( r_{\text{max}} \) is the maximum transmission range of nodes and have localization support. We denote the distance calculated from received signal strength (RSS) by \( d(u,v) \) and from location by \( ||u,v|| \) between two nodes \( u \) and \( v \). The set of neighbors of a node \( u \) is given by \( N(u) \). The path is denoted by \( p(u,v) \) between the nodes \( u \) and \( v \); which is the set of links constituting the route. In addition to sending and receiving messages, the radio communication provides signal strength. We assume that when node \( v \) receives a message \( m \) from node \( u \), it knows the reception power \( p_r \) of message \( m \). We assume that, given the transmission power \( p \) and the reception power \( p_r \), node \( u \) can estimate \( d(u,v) \).

For better realization of the problem, consider two attacking nodes that are present one hop far from gateway node and source node respectively. During gateway discovery, the attacking node which forms the wormhole, tunnels the gateway discovery messages it receives from neighbors, advertising false routes with lesser hop count. An adversary situated close to a gateway node may be able to completely disrupt the Internet access by creating well-placed wormholes. An adversary can convince the nodes which are multiple hops away from the gateway node that they are only one or two hops away via the wormhole. This can create a sinkhole, since the adversary on the other side of the wormhole can artificially provide a high quality route to the gateway, potentially all traffic in the surrounding area will be drawn through it if alternate routes are significantly less attractive.

3.1 Types of pseudo routes

Three geometric types of pseudo routes are presented. Fig. 2 shows the different types of pseudo route attack. Direct pseudo route attack occurs when both the ends of pseudo route are in the neighborhood of the gateway and the source node. Attacking nodes directly tunnel the gateway discovery packets from source to gateway node. Here, \( h(u,v) = 1 \) (refer Fig. 2 (a)). Semi-direct pseudo route occurs when one end of the pseudo route is in the neighborhood of gateway node (or in the neighborhood of the source node) and other end is any intermediate node in the route, but not in the neighborhood of either source or gateway node (otherwise, it becomes a direct pseudo route). Here, \( h(u,v) \geq 2 \) (refer Fig. 2 (b)). Indirect pseudo route occurs when none of ends of pseudo route are in the neighborhood of either gateway node or source node i.e., any two nodes in the route can be creating pseudo routes; except the nodes in the neighborhood. Here, \( h(u,v) \geq 3 \) (refer Fig. 2 (c)).
3.2 Proposed Architecture

The proposed solution identifies pseudo routes and rejects such routes during gateway discovery where the threat acts as a deterrent. Three factors are considered during design of protocol to mitigate the affect of pseudo route. The first one is support from signal strength measurement to find distance with neighbors. Since signal strength is determined by the receiver node, no node can advertise false information of its distance with neighbors. A node can measure its distance to another node using received signal strength since decay of the signal strength depends on the medium[10]. We use received signal strength as its measurement depends on the receiver. Since the attenuation of signal depends on the medium, nodes can not perform false advertisement of signal strength information unlike localization information [6]. The second one is support from localization information. There are many location supporting developed for MANET [12]. The third one is support from the unique pairwise key distribution between the gateway and nodes in the network. The protocol relies upon shared pairwise key distribution between the gateway and nodes in the network. The idea behind the shared key concept is preventing the manipulation of the contents that are piggybacked into the gateway verification packet; by intermediate nodes causing pseudo routes.

Let us first present an outline of the algorithm. All nodes in the network periodically broadcast hello() packets. Using signal strength measurements, nodes maintain a Neighbor Table (NT) containing neighbors entries with distances. As a first step, nodes check whether a node present in the route as neighbor is actually present in NT; acting as the first step to countermeasure the pseudo route attack. The node computes the average of the distances to the neighboring nodes, termed as hop cost. The nodes in the route piggyback own location and hop cost during the gateway verification (which will be discussed later) phase after gateway discovery. Based upon hop-cost and the locations information obtained through the gateway verification phase, gateway node checks if the route contains wormholes. On finding wormhole, the route is discarded and the source node is informed through a discard message.

The four types of messages exchanged by nodes are:
- hello(): Periodic neighbor discovery message (not encrypted).
- discard(): Message sent by gateway to source nodes about presence of pseudo route during gateway verification (encrypted).
- accept(): Unicast message sent by gateway to source nodes about absence of pseudo route during gateway verification (encrypted).
- discovery(): Gateway discovery message (not encrypted).

We consider three communication primitives: broadcast, send, and receive, defined as follows:
- bcast(u, p, m) is invoked by a node u to send a message m with power p; it results in all nodes in the set \{v|p(d(u, v)) ≤ p\} receiving m.
- send(u, p, m, v) is invoked by node u to sent message m to v with power p. This primitive is used to send unicast messages, i.e., point-to-point messages.
- recv(u, m, v) is used by u to receive message m from v.

3.3 Algorithm

There are two components of the protocol. The first one is for the periodic maintenance of the neighborhood information and executed by all the nodes in the network. The second component is initiated by the source nodes in the network during the gateway discovery phase.

3.4 Neighbor maintenance algorithm

All the nodes periodically broadcast hello() packets. But hello() packets themselves are vulnerable to wormhole attack. We have handles one-hop routes carefully by maintaining an interval at which hello() packets are broadcasted. This step is explained in details in Section 3.6. The neighboring nodes piggyback its location in the hello() packets. To store neighbor information, each node has a Neighbor Table (NT) to record active neighbor information. The NT records distance from each active neighbor to itself, both from location as well as through received signal strength.
In this phase, if a node receives a gateway discovery message from a node one hop far, it checks whether the node is present in the NT. If the node is not present in the NT, no route is established through that node. It works as the first step for the prevention for the pseudo routes. The idea behind the construction of NT is to discard such routes where a node is present as one hop neighbor but not present in neighbor table, NT; as a first measure to mitigate the affects of the pseudo route attack. Based upon the distance measurements, two parameters are defined. The first one is hop-cost, which is the average of the distances to the neighbors and the second one is mean hop-cost. They are as follows:

- **Hop-cost** of a node $u$ is the average of the distances (calculated from received signal strength) to set of nodes that are present within its transmission range, i.e., $N(u)$. It is denoted by $\eta(u)$ and given by $\frac{1}{|N(u)|} \sum_{w \in N(u)} d(u, w)$.
- **Mean hop-cost**: Mean hop-cost of two nodes $u$ and $v$, is calculated as: $\pi(u, v) = (\eta(u) + \eta(v))/2$.

The algorithm relies on hop-cost calculation. It can not rely on location information provided by neighbors since location information broadcasted by neighbors can be false. With each update of NT, the nodes recalculate hop-cost. In case of tunneling, when a node tunnels messages between neighbors, then the neighboring nodes hears two simultaneous `hello()` messages. If a node hears two simultaneous `hello()` messages in time less than the `hello()` packet broadcast interval, the node makes the entry invalid in NT but keeps the entry. As shown in Fig. 3, if a node broadcasts, and if a tunnel is present, the neighbor on the other side of the tunnel hears two broadcasts within the interval less than the broadcast timer one.

To ensure correct received signal strength, special measures are taken. This work assumes that all nodes know its maximum transmission range, $r_{max}$. Using $r_{max}$, the node calculates minimum receive power, $p_r(r_{max})$. Node knows maximum and minimum possible receive power. Further, gateway discovery protocol requires [9] bidirectional links. No route is established with unidirectional links [9]. For all nodes from which it receives `hello()` message, it compares the received signal strength with the minimum possible receive signal strength calculated based upon $r_{max}$. If it is smaller for any nodes, discard the node from NT. Thus, if a node attempts to deviate from the standard signal strength, it is not accepted as a neighbor and consequently no route through that node is established.

### 3.5 Gateway verification phase

This phase, called *gateway verification phase* is initiated after the source node finds a route to the gateway node through the gateway discovery phase. After the source node receives the route to gateway, it sends a gateway verification packet to the gateway node through the same route. In this phase, the source node piggybacks its location information as well as the hop-cost in the gateway verification packet. The message sent is encrypted using the key shared with the gateway node. While the gateway verification packet is sent through the same route, all the intermediate nodes in the route also piggyback its location information and the hop-cost in the gateway verification packet in an encrypted manner. Fig. 4 shows the same idea where node $w$ piggybacks by encrypting with the key shared by $w$ and $u$ where $u$ is the gateway node. The source node performing gateway verification phase decides to accept the route based on the message received within a bounded time from the gateway node. If the source node do not receive any reply within the bounded time or receives a `discard()` message, it discards the route. Otherwise, the source node accepts the route.

After the gateway node receives the location and $\eta(u)$ of all the intermediate nodes $u$, it runs the validity check for the route. Next, the condition used by the gateway node to decide the validity of a route is explained:

![Figure 4. When the gateway verification packet reaches a node $w$, it inserts its location and hop-cost by encrypting it with the key $(w, u)$. Here, $u$ is the gateway node.](image)

Consider an ideal path and a practical path between two nodes. The sum of distances among all the nodes constituting the links for the realistic route is higher than the ideal one. The sum of distances among the nodes of each link of path $p(u, v)$ is given by $\tau(u, v) = \sum_{i,j \in p(u, v)} ||i,j||$. In the case of an ideal path, $\tau(u, v) = ||u, v||$. The relationship between the realistic and the ideal path is $\tau(u, v) > ||u, v||$. This forms the basis for the protocol proposed in this work.

The approximate sum of distances between the nodes of each link along the route between the nodes $u$ and $v$ is denoted by $\sigma(u, v)$. The parameter $\sigma(u, v)$ is used as an approximation of $\tau(u, v)$. The value of $\sigma(u, v)$ is given by: $\sigma(u, v) \approx \pi(u, v) \times h(u, v)$. Further, $\sigma(u, v) = ||u, v|| + \tau$ where $\tau$ is the deviation from the ideal route. If the route to gateway during the Internet access gets trapped in a pseudo route, then by observing $\sigma(u, v)$ with respect to the geometric distance $||u, v||$, we can detect pseudo route attack.

A simple observation is derived that the sum of distances between the nodes of each link along a route is always greater than or equal to the geometric distance between the source and destination when there is no wormhole, i.e., $\sigma(u, v) \geq ||u, v||$. This condition is used by the gateway to detect pseudo routes. Motivated by this fact, our work is based on the assumption that the condition $\tau > 0$ always holds true for good routes. Based on this, the gateway node checks if $\tau < 0$ for every pair of combinations of nodes present in the route. So, given a route of $k$ nodes, $\binom{k}{2}$ route segments needs to be checked. If the condition $\tau < 0$ holds true for any pair of node in the routing path, then gateway node discards the route by informing the source node through `discard()` message. So, based on the above condition, we can eliminate the pseudo routes.

For a route of set of nodes $P_k(u, v) = \{u_1, u_i, \cdots, u_k\}$, which is found to be the best through the routing race condition, we check the pseudo route presence in all the combination of $\binom{k}{2}$ route segments. We check $\forall i, j \in P_k(u, v)$ if $\sigma(i, j) < ||i, j||$. If this holds true for any $i, j$, then the gateway sends a `discard()` message along the same route to the source node. If the message is not received by the source node after the timeout period, the source node automatically discards the route. Fig. 5 gives the basic pseudo route elimination algorithm.
Algorithm ELIMINATION()
1: Generate \((\frac{L}{2})^2\) route segments.
2: while \(\exists\) route segment \(r(i,j) \in (\frac{L}{2})^2\) do
3: \(\pi(i,j) \leftarrow \eta(i) + \eta(j)/2\)
4: \(\sigma(i,j) \leftarrow h(i,j) \times \pi(i,j)\)
5: if \((\sigma(i,j) \leq ||r(i,j)||)\)
6: \(send(u, discard(v))\) and record the attackers
7: end if
8: end while
9: \(send(u, accept(v))\)

Figure 5. The algorithm used by the gateway node after receiving the gateway verification packet.

3.6 Problem with one hop routes

To address the problem of hello() packet tunneling and well to take into account the problem of one hop routes, we treat one hop cases differently. Another factor that contributes to is radio irregularity. To ensure guaranteed connectivity between gateway and source node, the gateway node forms a region around itself; called as guaranteed presence region. It is the circular region of radius \(\eta(u)\) for node \(u\). Pseudo routes are easily detectable when \(||u, v|| > r_{max}\) due to violation of communication constraint. But when \(||u, v|| < r_{max}\), it needs special handling. The factor that complicates the second case is due to the error in range measurements caused by radio irregularity.

When the node is inside guaranteed presence region: In this step, first it is checked whether the distance of the source node computed from the localization reading is within the guaranteed presence region, i.e., \(||u, v|| < \eta(u)\). It also requires that the distance between the gateway node and the source node computed from signal strength is also within the guaranteed presence region, i.e., \(d(u, v) < \eta(u, v)\). If the distance of a neighbor computed from the localization reading is within the guaranteed presence region, there is no pseudo route.

Source node is outside the guaranteed presence region: If a node is not present within the guaranteed presence region and distance calculated from the localization readings is within the maximum transmission region, then this checking is required. Summing up, the condition is \(\eta(u) < ||u, v|| > r_{max}\). Similarly, for the distance calculated from the signal strength, the condition is \(\eta(u) < d(u, v) > r_{max}\). Otherwise, if \(||u, v|| < \eta(u)\) and \(d(u, v) < \eta(u, v)\) with \(h(u, v) = 1\), then there is no pseudo route. In this case, the gateway broadcasts the source node asking the neighbors whether any neighbor has an invalid entry for the source node. If any node replies with a positive response, the node declares the route as a pseudo route.

4 Experimental Results

We have developed a simulator using C++. CSMA/CA behavior is simulated among the nodes by not allowing a node to broadcast if it hears a broadcast message from another node within its transmission region. Few important parameters are namely, transmission radius of mobile devices (50 m), a geometric area of dimension \((500m \times 500m)\) containing 200 randomly distributed nodes. To introduce the metrics for evaluation of the proposed scheme, two new variables are introduced: \(r(u, v)\)(1 if the route between \(u\) and \(v\) is a pseudo route and otherwise 0) and \(R\) (the set of all the routes that are generated).

- **Effected route ratio** is the ratio of the number of pseudo routes to the total number of routes generated in the network. It is given by: \(\frac{\sum_{(u,v) \in R} r(u,v)}{|R|}\).
- **Classification percentage** is the ratio of the total number of routes correctly classified as the pseudo route to the total number pseudo routes generated. It is given by: \(\frac{\sum_{(u,v) \in R} r(u,v)}{\sum_{(u,v) \in R} r(u,v)}\).

4.1 Variation due to wormhole placement

Fig. 6 shows the variations of affected route ratio for different locations of the gateway. Let us first consider the case when the gateway is at center of the network. Among two malicious nodes forming the wormhole, one node is at the neighborhood of the gateway and the location of the other node is varied across the network. The affect is more severe when the other node creates the pseudo route close to the center of the network. Moreover, at few points, the more routes are affected when the node that creates the pseudo route is in the denser part of the network.

![Figure 6. The impact of the pseudo route attack is shown when the gateway is located at the center of the network and at the corner of the network.](image)

In Fig. 6, we have also evaluated the performance of the network where the gateway is at the corner of the network. Similar to the previous case, among the two nodes launching the pseudo route attack, one node is at the neighborhood of the gateway and the location of the other node is varied diagonally across the network. The results reflect that the affect on the Internet access is severe when the source node is also located close to the corner of the network. The affect is more disastrous than the case where the gateway node is at the center of the network. We can conclude that the affect of the pseudo problem is severe when the nodes forming the pseudo route are close with one end of the wormhole near the gateway.

4.2 Classification success

Fig. 7 shows the performance of the protocol in terms of classification percentage. Among the two nodes creating the pseudo
route, one is in the neighborhood of the gateway and the other node is fixed at the center of the network. We have plotted the classification percentage against the number of hops between the gateway node and the source node. It has been found that for the number of hops greater than 4, the success ratio of the protocol is 100%. In Fig. 7, for the hop count of 1 and 2, there is no problem of pseudo route. The special conditions for one hop routes handle such scenario.

4.3 Impact of network density

The influence of network density on impact of pseudo route is evaluated through the parameter affected route ratio. Two cases of gateway node location are considered: one at the center of the network and another at the corner of the network. In Fig. 8 (a), we have considered the case when the gateway node is at the center of the network. We have varied the number of nodes from 250 to 500 nodes in the network. Whereas 250 nodes represent a medium density network, 500 nodes represents a high density network. We can observe that network density do not affect the impact of pseudo route on affected route ratio (packet delivery). The impact on routing is significant when the other end of the wormhole is close to the gateway, i.e., the case of locations (200, 200) and (300, 300).

In another case (Fig. 8 (b)), the case of gateway node location at the corner of the network is evaluated. Compared to the case of gateway node location at the center, the impact of wormhole is more significant when the gateway is at the corner of the network rather than at the center. Similar to the previous case, we have varied the number of nodes from 250 to 500 in the network. We can observe that network density do not affect the impact of pseudo routes. The impact on routing is significant when the other end of the wormhole is closest to the gateway.

5 Conclusions and Future Work

We have presented the security issues associated with the Internet access from MANET and address the vulnerability of gateway discovery mechanism. We have systematically and comprehensively investigated the pseudo route attack, the generalized version of the wormhole attack. We have identified different types of pseudo route attack, classified them into three geometric groups. A simple and low overhead technique at different levels for detecting and mitigating misleading behavior introduced by pseudo routes is presented. Experiments reveal non-trivial facts about pseudo routes and possible impact on the performance of the protocol. As a part of the future work, we will test the described scheme in real platform and explore its use in sensor networks.

References