Towards Secure Multi-path Routing for Wireless Mobile Ad-Hoc Networks: A Cross-layer Strategy

Arjun P. Athreya and Patrick Tague
{*arjun.athreya, patrick.tague*}*@sv.cmu.edu*
Wireless Network and System Security Group
Electrical and Computer Engineering
Carnegie Mellon University, USA

***Abstract*—Multi-path routing establishes multiple paths between a source and destination node in a network. This helps in achieving reliability in mobile ad-hoc networks (MANETs). To achieve efficient, secure and reliable multi-path routing for MANETs, we propose a routing mechanism that uses cross-layer strategies. The cross-layer strategy involves incorporating feedback and information from layers below the network layer to make decisions at the network layer. We also propose a path evaluation mechanism for the paths returned by the proposed multi-path routing mechanism.**

I. Introduction

MANETs demand end-to-end reliability guarantees in routing operations. With high mobility, once-established links could fail which lead to communication failures. One possible solution to this problem is to have multi-path routing capabilities in MANETs. Multi-path routing establishes multiple paths between particular source and destination network nodes. This helps in achieving reliability in MANETs apart from other benefits such as load balancing [1].

In theory, completely disjoint paths between source and destination nodes are required to maximize the benefits of multi-path routing. In practice, this is very hard if certain nodes in a partitioned network act as gateway nodes to another set of nodes. Hence, current research has focused on establishing maximally disjoint paths between particular source and destination nodes [1].

An application for secure multi-path routing is, critical messages being securely and reliably delivered among soldiers treading a hostile environment.

In this paper, we propose a cross-layer strategy for secure multi-path routing in MANETs. The routing decisions made at the network layer depend on feedback and inputs from the lower physical and link layers. Security is built into this routing mechanism and path selection is based on forwarding behaviors of nodes in the network and link quality of each hop in a path. We show that with mobile nodes, cross-layer strategy via information sharing from lower layers helps in achieving reliability in routing and path selection.

We discuss the system model and assumptions in Section II and introduce the multi-path routing using cross-layer strategies in Section III. Section IV discusses securing the proposed multi-path routing and path evaluation is discussed in Section V . We discuss our future work and conclude in Section VI.

II. System model and assumptions

The network is an undirected graph $G = (N, E)$, where N represents nodes in the network and E represents the links between the nodes in the network. Nodes in the network support unicast and broadcast communications.

The paths established between a source and destination node pair $S, D \in N$ is denoted by the set P_{SD}. We assume that the network is deployed by one entity or an enterprise and the network nodes have pairwise symmetric keys installed in them. K_{ij} denotes the shared symmetric-key between nodes i and j. The nodes periodically broadcast beacons which contain their identity and other programmed information. Nodes do not cache any previously established routes and do not perform gratuitous route replies to route request messages. Destination node acknowledges on receiving a packet successfully and the acknowledgement packet contains the source route on which data packet was received or the ID of the route. We also assume that node's hardware is tamper proof.

A. Adversary model

As nodes are deployed by one entity, we have in-network adversaries. This adversary can drop packets, provide false updates, spoof network packets, launch black-hole attack and DoS attacks through broadcast storms. The adversary could exhibit an ON-OFF behavior being selective in its participation in network control operations and abstain from data forwarding.

III. Multipath routing using a cross-layer strategy

In this section we introduce and explain the multi-path routing mechanism using a cross-layer strategy, allowing for routing decisions to be made based on information gathered from the physical and link layers.

A. Node neighborhood using physical layer measurements

One of the assumptions stated in Section II is, periodic beaconing in the network conveying their presence in the network. This enables network nodes in their radio proximity to be aware of who their neighbors are. In our paper we define neighborhood N_i of any node $i \in N$ as a set of network nodes $j \in N$, who's beacon's received signal strength indication (RSSI) is greater than a preset threshold and consistent over at-least p beacon periods.

If mobile nodes move across neighborhoods in each beacon period, then immediate neighborhood update will be inconsistent with actual neighborhood. This notion of stationarity in network dynamics help in building reliability and consistency in data required for network layer operations.

The use of RSSI for neighbor-aware networking in MANETs has been well explored [2] [3]. Through beaconing, nodes share their *connectivity information*. We define *connectivity information* as a set of nodes in the network who are immediate neighbors or reachable via the neighboring node being on the path. If mobility in nodes lead to change in neighborhoods, the nodes update their connectivity information via their beacons. From the *small world* model [4] [5], it can be assumed that certain nodes in a network will continue to have good connectivity even when nodes are mobile. Analogy to this would be, soldiers at the edge of the pack may not have consistent neighbors compared to soldiers in the middle of the pack. It is fair to assume that network nodes on deployment first establish their neighborhood prior to establishing any path in the network.

B. Route establishment

Source node $S \in N$ wants to reach the destination node $D \in N$. At first, S checks if D is its one hop neighbor, in that case no route establishment is needed, the message is sent across to D by unicasting it. However, if D happens to be reachable via nodes $m \in N_S$, then S unicasts the *route request* (*rreq*) packet(s) with D as the destination and first hop as the neighboring node(s) that have connectivity to D.

An intermediate node on receiving a *rreq* packet performs the same operation that the source node performs if it finds that its neighbors can reach D. At each hop the nodes add their next hop neighbor whom they know can reach D. In this process, the nodes check if they have received multiple copies on the same path by validating a random nonce. They do not discard the *rreq* packets coming from different paths, this is to support maximum number of paths to be established between a source and destination. If a node sees itself listed in the path, it drops the *rreq* packet and looping is avoided.

S or the intermediate nodes may not have any connectivity to D even through its neighbors. D may have moved, its new neighborhoods are not updated yet and its previous neighborhoods have no connectivity to D. In this case, the *rreq* packet is broadcasted. The broadcast will stop at a neighborhood that is updated about D's connectivity. Thus beaconing helps in mitigating *rreq* packet's broadcast storm to some extent.

Once the *route request* packet reaches D, it constructs a *route reply* (*rrep*) packet and sends it back to S in the same path it was received. The destination node D does this for all *rreq* packets it receives from different routes. If the intermediate nodes receive a *rrep* message, D's ID is added to the list of nodes in their connectivity list. This connectivity information is updated in their next beacon.

C. Route management

When a node in a path knows that connectivity to the next hop node in the network is lost during data forwarding, it creates a gratuitous *rreq* packet and broadcasts it to its neighborhood. The new *rreq* packet carries with it the original forwarded message from S destined to D as a payload. Eventually the gratuitous *rreq* message reaches D using route establishment mechanism in Section III-B. D processes the request message and the forwarded data packet, constructs a new acknowledgement packet that informs S not only of data being acknowledged, but also of a new route S could consider for routing data.

The intermediate nodes which see the link failure do not broadcast a *link failure* message, but rather update their neighborhood of the connectivity information by deleting the entry of D in their connectivity list through their periodic beacons. Thus link failures are reported in a subtle, but very efficient manner. Compared to traditional MANET routing protocols [6] [7], we have proposed a source routing mechanism that uses the knowledge of network node's connectivity. With time, it is possible that every node in the network has connectivity information to every other node.

D. Link layer measurements for path reliability

In the *rrep* packet, each intermediate node in the path adds a measurement observed in the link layer. Estimated Transmission Count (ETX) is a measurement from the link layer which is reported to the network layer through the *rrep* packet [8]. When S processes this information, it has a notion of how good the intermediate links of the path p_{SD} are.

IV. Security for multi-path routing in MANETs

The communications between S and D are authenticated by verifying a nonce (η_S) sent by S. Since we are in the realm of multi-path routing, we aim to reduce the cryptographic computations as more packets might have to be processed compared to uni-path routing.

When S wants to send a data packet or initiate a $rreq$ process, it sends a nonce in the clear and also encrypts the nonce with the path using the shared symmetric key with the destination as shown in Figure 1. In subsequent hops, the intermediate nodes encrypt the nonce and append their ID with encrypted payload from previous node and encrypt this whole message with the share symmetric key between them and D. On receiving this message, D decrypts the packet in the reverse order of the ID's recorded in clear text and verifies the nonce sent by S with the decrypted version of the nonce sent by all intermediate nodes. If they all match, then the destination believes that packet has arrived from S, intermediate nodes have participated correctly in the forwarding or route establishment phase and the message has traversed in the same path as declared by S. The proposed multi-path routing mechanism explained in Section III along with security features is shown in Figure 1.

A. Countering adversarial behavior

Since D securely acknowledges every communication made by S, S maintains the forwarding behavior of the intermediate nodes on the path to D. The forwarding behavior of a node is

\\ **Route Discovery**
\\ S wants to reach D
if $D \in N_S$
$S \rightarrow D : \langle S, D, \eta_S, \{\eta_S, TS_S, Data\}_{K_{SD}} \rangle$
else if $D \in N_S$'s connectivity
$\forall j \in N_S$with connectivity to D
$S \rightarrow j : \langle S, j, D\{j, \eta_S, \{S, D, TS_S, \eta_S\}_{K_{SD}}\}_{K_{Sj}} \rangle$
else
$S \rightarrow * : \langle S, D, \eta_S, \{S, D, TS, \eta_S\}_{K_{SD}} \rangle$
end if

\\ Intermediate node j receives the *rreq* packet to D
if message request is not fresh and from the same path
Drop request
else if $D \in N_j$
$j \rightarrow D : \langle S, j, D, \eta_S, \{\eta_S\}_{K_{jD}}, \{S, D, TS_S, \eta_S\}_{K_{SD}} \rangle$
else if $D \in$ any of N_j's connectivity
$\forall k \in N_j$ with connectivity to D
$j \rightarrow k : \langle S, j, k, D, \eta_S, \{j, k, \eta_S, \{\eta_S\}_{K_{jD}}, \{S, D, TS_S, \eta_S\}_{K_{SD}}\}_{K_{jk}} \rangle$
else Re-broadcast source's request
$j \rightarrow * : \langle S, j, D, \eta_S, \{\eta_S\}_{K_{jD}}, \{j\{S, D, TS, \eta_S\}_{K_{SD}}\}_{K_{jD}} \rangle$
end if

\\ node j sees break in link to next-hop node in source route
if no connectivity to D in N_j
$j \rightarrow * : \langle S, \ldots, j, D, \eta_S, \{\{\eta_S, TS_S, Data\}_{K_{SD}}\}_{K_{jD}} \rangle$
else if $\forall i \in \eta_j$ has connectivity to D
$j \rightarrow i : \langle S, .., j, i, D, \eta_S, \{j, i, \eta_S, \{\eta_S, \}_{K_{jD}}, \{\eta_S, TS_S, Data\}_{K_{SD}}\}_{K_{ji}} \rangle$
end if
D processes $rreq$ and constructs a $rrep$ packet
$D \rightarrow$ last hop node on source route : $\langle$Reversed Source Route $\{$Source Route, $\eta_S, TS\}_{K_{SD}} \rangle$

Fig 1. This figure explains the secure multi-path routing mechanism using cross-layer strategy. $i \rightarrow j$ and $i \rightarrow *$ denote node-node communication and broadcast communication respectively.

a ratio of successfully acknowledged packets to total number of packets routed through that node, this also serves as a reputation metric. If the acknowledgement is lost or is incorrectly acknowledged, the reputation value for intermediate nodes drop. Adversary nodes cannot modify the original *rreq* packet or inject additional information as η_S is encrypted with K_{SD} which is known only to S and D. If tampered, D will see that the nonce test fails. Black-holing cannot be avoided during network bootstrapping phase, but once network node connectivity information is established black-holing could be mitigated. Broadcast storms are mitigated by network nodes sharing updates using beacons.

V. Path evaluation process

Each intermediate node appends the probability distribution of the ETX measurements for its next hop neighbor in the *rrep* packet. Each ETX measurement is treated as an independent random variable denoted by ETX_{ij}, with a probability distribution of finite mean and variance denoted by $P_{E_{ij}}$. Forwarding history of each intermediate node (F_i) on the obtained path can also be treated as an independent random variable with a distribution (P_{F_i}) which has finite mean and variance. We assume that there is a trustworthy process in place to compute and collect the ETX and forwarding statistics.

If the independent random variables are identical in their distribution, Central Limit Theorem (CLT) can be used to derive the average ETX (ETX_p) and forwarding statistics (F_p) of a path p. Using (1) and (2), it can be seen that a random variables ETX_p and F_p are be defined as sum of respective independent random variables.

$$ETX_p = \sum_{\text{link } ij \in p} ETX_{ij} \tag{1}$$

$$F_p = \sum_{\text{link } ij \in p} F_i \tag{2}$$

We formulate he utility function U_p of p as a function of ETX_P and F_p represented as $U_p = f\,(ETX_p\,,\, F_p)$. If the resulting distribution of U_p is Gaussian, then it helps us in determining the extent of reliability in a path p. Thus, even if nodes keep track of round trip time of messages for the path itself, they will be able to better estimate the quality of path using this utility function which even incorporates link quality.

VI. Conclusion and future work

The cross-layer strategy in our paper is to use RSSI measurements in the physical layer to define node neighborhood, ETX measurement from the link layer and node forwarding behavior from network layer to study path reliability via a utility function. We use all these as building blocks to support reliable and secure multi-path routing via a cross-layer strategy. We intend to simulate the proposed mechanism and study the effects of traditional MANETs security attacks on multi-path routing.

References

[1] S. Mueller, R. Tsang, and D. Ghosal, "Multipath routing in mobile ad hoc networks: Issues and challenges," in *Performance Tools and Applications to Networked Systems*, ser. Lecture Notes in Computer Science, M. Calzarossa and E. Gelenbe, Eds. Springer Berlin Heidelberg, 2004, vol. 2965, pp. 209–234.

[2] A. Savvides, C.-C. Han, and M. B. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the 7th annual international conference on Mobile computing and networking*, ser. MobiCom '01. New York, NY, USA: ACM, 2001, pp. 166–179.

[3] M. Sichitiu and V. Ramadurai, "Localization of wireless sensor networks with a mobile beacon," in *Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on*, oct. 2004, pp. 174 – 183.

[4] A.-L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[5] D. J. WATTS, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440–442, 1998.

[6] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," *Mobile Computing Systems and Applications, IEEE Workshop on*, vol. 0, p. 90, 1999.

[7] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, ser. The Kluwer International Series in Engineering and Computer Science, T. Imielinski and H. F. Korth, Eds. Springer US, 1996, vol. 353, pp. 153–181.

[8] S. M. Das, H. Pucha, K. Papagiannaki, and Y. C. Hu, "Studying wireless routing link metric dynamics," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, ser. IMC '07. New York, NY, USA: ACM, 2007, pp. 327–332.