A Literature Survey of Secure Route Discovery Schemes in MANET

Ajay Dureja[1], Vandna Dahiya[2]
[1]PDM College of Engineering for Women , Bahadurgarh (Haryana)
[2]PDM College of Engineering for Women, Bahadurgarh (Haryana)

Abstract- **Having a secured transmission and communication in MANET is a challenging and vital issue as there are various types of attacks that the mobile network is open to. In order to secure communication in such networks, developing schemes to secure the routing is a great task and concern. Various techniques have been proposed with varying flavors of security, efficiency and robustness in MANETs. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Here we focus on the study of securing the route discovery schemes in MANET.**

Keywords: MANET, Route Discovery, FRESH, SRDP, AODV

I. INTRODUCTION

MANETs suffer from a variety of security attacks and threats such as: Denial of Service (DoS), flooding attack, impersonation attack, selfish node misbehaving, routing table overflow attack, wormhole attack, blackhole attack etc. MANET is open to vulnerabilities as a result of its basic characteristics like no point of network management; topology changes vigorously, resource restriction, no certificate authority or centralized authority.

Routing protocols for mobile ad hoc networks generate a large amount of control traffic when node mobility causes link states and the network topology to change frequently. On the other hand, resources such as bandwidth and battery power are usually severely constrained in such networks. Therefore, minimizing the control traffic to set up and maintain routing state is one of the main challenges in the design of scalable routing protocols for mobile ad hoc networks. One approach to limit control traffic is to establish routes on demand rather than proactively. On-demand routing protocols [1] only establish a route to a destination when it is necessary to send packets to that destination, and therefore incur less overhead at the expense of higher route setup latency. Hybrid routing protocols [1],[2] combine both on-demand and proactive elements for more edibility in the latency-overhead trade. On-demand routing overhead can be broken down into two components: route discovery and route maintenance. In AODV, whenever a source S needs to communicate with a destination D, it checks for an existing route to D in the routing table. If the route is not present, it initiates a route discovery by broadcasting a RREQ (Route Request) packet which is flooded [3] into the network in a controlled manner, until it reaches the destination or until it reaches a node, which knows a route to the destination. Then, the destination or an intermediate node sends back a Route Reply (RREP) message, which includes the number of hops in between. Each node receiving the RREP message records a forward route to the destination and, thus, knows only the next hop required for a given route.

Like most network protocols, MANET routing protocols are often designed for non-adversarial networks and thus forgo security features. This follows the traditional model of first designing a protocol and later (sometimes much later) retrofitting it with security features. Being a popular protocol, DSR has received a lot of attention from the security community. The state-of-the art of MANET routing security is represented by Ariadne [4,5,6] which is a DSR-specific security mechanism based on the earlier TESLA protocol [7]. Ariadne's security is based on message authentication codes (MACs) and loose time synchronization among nodes is required.

The critical issue for routing in mobile ad hoc network is how to select a stable path with longer lifetime since mobility and power drain of a node causes frequent path failure. This path failure causes frequent route discovery which affects the performance of the routing protocol. The path failure also increases computational overhead of the nodes.

The remainder of the paper is organized as follows.
Section 2 states the idea behind the route discovery scheme. Section 3 states basic challenges in discovering the route . Section 4,5,6 reviews some of the route discovery schemes. Section 7 concludes this paper.

II. ROUTE DISCOVERY IN MANET

MANET is infrastructure less network. Each node can perform the role of a host as well as a router. Hence the nodes which are out of transmission range can be accessed by routing through intermediate nodes. Often, hosts in a MANET operate with limited batteries and can roam freely towards any direction at any speed.

The power exhaustion of some nodes and the mobility nature of nodes cause frequent topology changes. So the path between nodes or group of nodes may change periodically. The node which wants to transmit data packets first needs to discover the route to the destination using route discovery process of different routing protocols. There are two kinds of routing protocols, one is reactive or on demand routing protocol, and another is proactive or table-driven routing protocol. In mobile ad hoc networks, a host may exhaust its power or move away without giving any notice to its cooperative nodes, causing changes in network topology, and thus these changes may significantly degrade the performance of the routing protocol. So the route needs to be discovered with longer route lifetime with fewer changes. As the route consists of number of wireless links, the route lifetime depends on the life time of nodes and individual links. The route discovery without considering the lifetime of the route leads to frequent failure and thereby to route discovery. As a result the computational overhead of the routing protocol increases considerably.

III. SECURE ROUTE DISCOVERY CHALLENGES

In this section, we observe that it is not possible to achieve secure route discovery in an MANET within a composable security framework that does not add in additional global and physical information, if the route sought is a simple path. However, before following this argument, it is important to note that there is no way of checking that a discovered route is not under the control of the adversary, because adversarial behavior is unpredictable. So, our argument is not about the impracticality of finding secure routes but the impracticality of finding paths that correspond to physical routes in the network. We base it on the fact that every route discovery algorithm is, in practice, vulnerable to attacks that exploit alternative communication channels. The purpose of routing being to establish a communication infrastructure, it is always reasonable to assume the existence of alternative communication channels, namely those that route discovery will establish. Even though it is not possible to discover secure routes in general MANETs, there are several other approaches that could be used to establish secure communication channels. Here we consider one approache: route discovery with traceability.

A. Route Discovery with Traceability

A practical solution would be to use routing algorithm that trace malicious behavior—see, e.g., [8]. It is possible to do this in such a way that there is practically no additional cost when the adversary is passive, while the extra cost is only for tracing adversarial nodes (optimistic tracing [8]). This approach supports self-healing security: The power of the adversary is diminished with each attack if we assume that the number of adversarial nodes is bounded over time.

IV. SECURE ROUTE DISCOVERY PROTOCOL (SRDP)

One approach is to perform ‘‘forward authentication” of route request (RREQ) packets as they propagate from the source to the destination. Each node can compute and add its authentication tag to the RREQ before re-broadcasting it. The main advantage of this approach is that it would allow the destination to authenticate the accumulated source route before it generates a RREP back towards the source. However, there are also some drawbacks or issues: a node that processes a RREQ packet has no assurance of being on the eventual route. In fact, in a large MANET, it is safe to say that many nodes that process a given RREQ will not be part of the route. Thus, computing an authentication tag can be wasteful for two reasons: computation that may wind up being unnecessary, and costs in terms of extra bandwidth. Second, even if the above is justified, the authentication tags must be eventually verified. This can be a very expensive procedure since each node in the route would authenticate a distinct route prefix. For example, given an actual route: S–B–C–D, node B would authenticate a route prefix S–B, node C would authenticate S–B–C, and so on. Third, we note that, if a particular sequence of nodes winds up forming a viable route, the destination generates a route reply (RREP) which then traverses the very same sequence of nodes in the reverse order. These issues motivate us to explore the alternative: ‘‘backward authentication” of RREP packets.[9] , [10]

Backward authentication is conceptually very simple: each node in the route ‘‘sees” the entire route as it processes the RREP packet. It can thus easily compute an authentication tag and append it to the packet. Moreover, an intermediate node can also perform a ‘‘sanity check” on the route by checking for anomalies, such as loops, routes that are too long or impossible according to its own cache, etc. When a RREP with a route of length t finally reaches the source, the latter can easily verify each tag and, if all tags are verified, conclude that all nodes’ view of the route is exactly the same. Therefore, any modification of the route as it propagates back in a sequence of RREP packets, is ultimately detected by the source. The only attacks not addressed are those caused by feedback loops and can be stated as follows-

(1) the adversary can delete from the route honest nodes that are ‘‘sandwiched” between a pair of compromised nodes, or (2) the adversary can add to the route a set of compromised nodes as long as it inserts them between a pair of other compromised nodes in the route. However,the adversary is unable to manipulate any honest nodes

in the route that are positioned outside any feedback loop.[11],[12]

V. FRESHER ENCOUNTER SEARCH (FRESH) ALGORITHM

Fresher Encounter Search (FRESH),[13],[14] a simple algorithm for efficient route discovery in mobile ad hoc net-works. Nodes keep a record of their most recent encounter times with all other nodes. Instead of searching for the destination, the source node searches for any intermediate node that encountered the destination more recently than did the source node itself. The intermediate node then searches for a node that encountered the destination yet more recently, and the procedure iterates until the destination is reached. Therefore, FRESH replaces the single network-wide search of current proposals with a succession of smaller searches, resulting in a cheaper route discovery. Routes obtained are loop-free. The performance[15] of such a scheme will depend on the nodes' mobility processes. It requires that nodes keep a table of their most recent encounter times with all other nodes. An encounter between
two nodes happens when those nodes are one-hop neighbors. Since one-hop neighborhood is dependent on the link layer, the exact condition for an encounter to occur will vary depending on the underlying wireless technology used.
The encounter age[16] of two nodes n and m is the time elapsed since the most recent encounter of n and m. Encounters can be detected by overhearing any packets (whether regular data packets, or purposely sent "Hello" packets) send by neighboring nodes, or they might be detected at the link layer, as in the case of Bluetooth.
The simple formulation of the FRESH algorithm can be described as follows-
Nodes keep a table of their most recent encounter times with all the nodes they have encountered. This table is queried by calling prevEncounterAge(NID), where NID is a unique node identifier, for example the node's IP address. prevEncounterAge(NID) returns a scalar representing the time elapsed since NID was last a one-hop neighbor, or 1 if NID has never been encountered. The pseudo-code below invokes the search primitive through an abstract interface which allows a querying node N to find the nearest anchor node A having seen the destination node D more recently than a time T. This search is invoked by calling findNextAnchor(D, T), which triggers a network search and returns A. In accordance with Definition 1 the search process creates routing state in the network which will allow N to subsequently send packets to A. This state will be used by the notifyNextAnchor call to instruct A to pursue the route discovery. More precisely, notifyNextAnchor(A,D) will send a packet to A, which triggers invocation of the call FRESH(D) on node A. We note that the packet sent by the notifyNextAnchor(A, D) call does not need to carry the time T representing the current node's encounter age with D since node A only needs its own encounter age with D in order to iterate the search. The algorithm, which is run at every node in the network, is as follows:

```
proc FRESH (D) = {
if (thisnode.ID = D) then {
replyToSource()
} else {
T := prevEncounterAge(D);
A := findNextAnchor (D, T);
if (A != D) then
notifyNextAnchor(A, D);
}
}
```

VI. ADJUSTED PROBABILISTIC FLOODING ON THE AD-HOC ON DEMAND DISTANCE VECTOR (AODV) PROTOCOL ALGORITHM

AODV is a well-known and widely studied algorithm which has been shown over the past few years to maintain an overall lower routing overhead compared to traditional proactive schemes, even though it uses flooding to propagate RREQs. Simulation results reveal that equipping AODV with fixed and adjusted probabilistic flooding, instead, helps reduce the overhead of the route discovery process whilst maintaining comparable performance levels in terms of saved rebroadcasts and reach ability as achieved by conventional AODV. Moreover, the results indicate that the adjusted probabilistic technique results in better performance compared to the fixed one for both of these metrics.

A probabilistic approach to flooding has been suggested in [17],[18],[19] as a means of reducing redundant rebroadcasts and alleviating the broadcast storm problem. In the probabilistic scheme, when receiving a broadcast message for the first time, a node rebroadcasts the message with a pre-determined probability p, thus, every node has the same probability to rebroadcast the message. When the probability is 100%, this scheme reduces to simple flooding. Studies [20] have shown that probabilistic broadcasts incur significantly lower overhead compared to blind flooding while maintaining a high degree of propagation for the broadcast messages. This paper focuses on evaluating the performance of our adjusted probabilistic flooding scheme by comparing it with the flooding technique of AODV as well as a fixed probabilistic approach. In routing algorithms such as AODV the use of a broadcast is to discover a particular destination node. As a consequence, a RREQ packet does not need to reach all the nodes in the network once a particular path has been discovered that leads to the desired destination. In this paper, we implement forwarding probabilities in a dynamic and fixed manner for on-demand route discovery process in a well-known on-demand routing protocol, namely AODV.

The adjusted rebroadcast probability[21] for probabilistic broadcasting algorithm for each node is briefly presented in Algorithm below which is a combination of the probabilistic and knowledge based approaches. It dynamically adjusts the re broadcast probability p at each mobile host according to the value of the local number of neighbors. The value of p changes when the host moves to a different neighborhood. In a sparser area, the rebroadcast probability is larger and in denser area, the probability is lower. Compared with the probabilistic approach where p is fixed, our algorithm achieves higher saved rebroadcast. Also, the decision to rebroadcast is made immediately after receiving a packet in the algorithm without any delay. By presenting an estimate of the average number of neighbors as the basis for the selection of the value of p. Let A be the area of an ad hoc network, N be the number of mobile hosts in the network.

Algorithm The adjusted probabilistic flooding algorithm on hearing a broadcast packet m at node X, n is average number of neighbor (threshold value) get degree n of a node X (number of neighbors).

if packet received for the first time then
if n < n then
node X has a low degree
set high rebroadcast probability p = p1
else
node X has a high degree
set low rebroadcast probability p = p2
end if
end if
generate a random number RN over [0, 1]
if RN ≤ p then
rebroadcast message
else
drop message
end if

The average number of neighbor can be obtained as shown below.

$$\mathbf{n = (N - 1) * 0.8 * \pi 2/A}$$

CONCLUSION

In this paper, we have summarized some of the secured route discovery schemes in an ad-hoc network and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of an ad-hoc networks require high degree of security on the other and ad hoc network are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks.

The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many both known and unknown security threats. Several other attempts have been made to address the security of MANET route discovery more robustly, the most recent one being introduced in a series of papers by Buttya`n and Vajda [12] and Acs et al. [13], [14], [15], [16]. In these works, the authors develop a formal idealization and simulation framework that adapts ideas from the secure reactive systems approach [17] and universally composable security approach [18] to the realm of MANET applications.

ACKNOWLEDGMENT

I would like to express my grateful thanks to all the authors whose work I referenced to during my review.

REFERENCES

[1]. X. Hu, J. Wang, and C. Wang, "Routing in Mobile AdHoc Networks," *IEEE conference*.
[2]. P. Albers et al., "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing TrustBased Approaches," 1st Int'l. Wksp. WL Info. Sys., 4th Int'l. Conf. Enterprise Info. Sys., 2002
[3]. L. Venkatraman and D. P. Agrawal, "Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks," J. Parallel Distrib. Comp., 2002.
[4]. G. Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," Technical Report 159, *Int'l Assoc. for Cryptologic Research*, 2004.
[5]. G. Acs, L. Buttya´n, and I. Vajda, "Provable Security of On- Demand Distance Vector Routing in Wireless Ad Hoc Networks," Proc. European Workshop *Security and Privacy in Ad Hoc and Sensor Networks* (ESAS '05), pp. 113-127, 2005.
[6]. G. Acs, L. Buttya´n, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," *IEEE Trans. Mobile Computing*, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.
[7]. [RY2009] Rai Tirthraj, Verma A K, "Survey and Analysis of Secure Routing Protocols for MANETs," in the proceeding of National Conference on *Cutting Edge Computer and Electronics Technology (CECT 2009), Pantnager, PP 501-06 in February 14- 6,2009.*
[8]. M. Burmester, T. van Le, and M. Weir, "Tracing Byzantine Faults in Ad Hoc Networks," Proc. Conf. *Computer, Network and Information Security* 2003, pp. 43-46, 2003.
[9]. W. Diffie, M.E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, 1976.
[10]. M. Bellare, R. Canetti, Hugo Krawczyk, "Keying Hash Functions for Message Authentication", Lecture Notes in Computer Science, 1996.
[11]. P. Papadimitratos, Z. Haas, "Secure routing for mobile ad hoc networks", in: *SCS Communication Networks and Distributed Systems Modelling Simulation Conference* CNDS, 2002.

[12]. Y.-C. Hu, A. Perrig, D.B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks", MOBICOM, 2002.
[13]. Charles E. Perkins and Elizabeth M. Royer. "Ad hoc on-demand distance vector routing." In Proceedings of the 2nd IEEE Workshop on *Mobile Computing Systems and Applications*, New Orleans, LA, February 1999.
[14]. Bluetooth SIG. Bluetooth v1.1 specification. *http://www.bluetooth.org*, 2000.
[15]. B. Williams and T. Camp. "Comparison of broadcasting techniques for mobile ad hoc networks". In Proceedings of the ACM International Symposium on *Mobile Ad Hoc Networking and Computing*(MOBIHOC), 2002.
[16]. Z. J. Haas M. R. Pearlman and T. Samar. "Zone routing protocol" (zrp). IETF, Internet-Draft, 2002.
[17]. Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu. "The broadcast storm problem in a mobile ad hoc Network". Wireless Networks, 8(2/3):153–167, 2002.
[18]. B. Williams and T. Camp. "Comparison of broadcasting techniques for mobile ad hoc networks". In MobiHoc '02: Proceedings of the 3rd ACM international symposium on *Mobile ad hoc networking & computing*, pages 194–205, New York, NY, USA, 2002. ACM Press.
[19]. D. C. Y. Sasson and A. Schiper. "Probabilistic broadcast for flooding in wireless mobile ad hoc networks". Technical Report IC/2002/54, *EPFL*, 2002.
[20]. Q. Zhang and D. Agrawal. "Dynamic probabilistic broadcasting in manets." Journal of *Parallel Distributed Computing*, 65:220–233, 2005.
[21]. W. Peng and X.-C. Lu. "On the reduction of broadcast redundancy in mobile ad hoc networks". In MobiHoc '00: Proceedings of the 1st ACM international symposium on *Mobile ad hoc networking & computing*, pages 129–130, Piscataway, NJ, USA, 2000. IEEE Press.