ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Advanced Security of Route Discovery in MANETs

G. Yedukondalu*, M. Srinivas, V. Kondala Rao# and R. RaviKumar
Asst.Prof & Asso.Prof #
CSE Dept, SBIT
Khammam , India
Yedukondalu8@gmail.com
minumula@yahoo.com
Vkrao1977@gmail.com
rachaswamy@yahoo.co.in

***Abstract**:* Mobile ad hoc networks (MANETs) are collections of wireless mobile devices with restricted broadcast range and resources, and no fixed infrastructure. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security points of view. A security model to the specific requirements of MANETs was introduced among the novel a characteristic of this security model is that it promises security guarantee under concurrent executions, a feature of distributed computation. A novel route discovery algorithm called endairA was introduced, together with a claimed security proof within the same model. In this paper, we show that the security proof for the route discovery algorithm, vulnerable to a hidden channel attack and the security framework.

Keywords: Network protocols: routing protocols, distributed networks, MANET security, hidden channels, provably secure protocols.

I. INTRODUCTION

Routing is a basic functionality for multihop mobile adhoc networks (MANETs). These networks are decentralized,with nodes acting both as hosts and as routers,forwarding packets for nodes that are not in transmissionrange of each other. Several route discovery algorithms have been proposed in the literature (see, e.g., [1], [2], [3],[4], [5]). These focus mainly on efficiency issues such accsalbulity with respect to network size, traffic load, mobility, and on the adaptability to network conditions such as link quality and power requirements. Some of the proposed routing algorithms also address security issues (e.g., [6], [7], [8], [9], [10], for a survey, see [11]), but their security is restricted to rather weak adversary models. There are several reasons for this, he most important one being that it is hard to model a formal security framework that captures all the basic security aspects of a MANET.

II. ROUTING ALGORITHMS

Routing is a basic network functionality that supports communication. In MANETs, each node acts as a router forwarding data to other nodes. We distinguish three basic phases in routing: 1) route discovery in which one or more routes (of adjacent nodes) that link a source S to a target T are sought, 2) route maintenance in which broken links of established routes are fixed, and 3) packet forwarding in which communication is achieved via established routes. Route discovery can be proactive or reactive (on-demand). Proactive routing is usually table driven: nodes maintain routing tables with routing information to potential target nodes. The tables are updated at regular intervals and used by intermediate nodes for route discovery. With reactive algorithms, routes are discovered only when needed. Source-initiated on-demand route discovery is triggered

by a node that requests from its neighbors information that can be used to find a route that links it to a target node. The neighbors forward the request to their neighbors, and so on, until a route that links S to T is discovered.

A. *The Source Routing Protocol (SRP):*

SRP [3] is an on-demand source routing protocol that captures the basic features of reactive routing. In SRP, route requests generated by a source S are protected by Message Authentication Codes (MACs) computed using a key shared with the target T. Requests are broadcast to all the neighbors of S. Each neighbor that receives a request for the first time appends its identifier to the request and rebroadcasts it. Intermediate nodes do the same. The MAC in the request is not checked because only S and T know the key used to compute it. When this request reaches the target T, its MAC is checked by T. If it is valid, then it is assumed by the target that all adjacent pairs of nodes on the path of the route request are neighbors. Such paths are called valid or plausible routes. The target T replaces the MAC of a valid route request with an MAC computed with the same key that authenticates the route. This is then sent back (upstream) to S using the reverse route. For example, a route request that reaches an intermediate node Xj is of the form msgS;T;rreq ¼ rreq; S; T; id; sn;X1; . . .;Xj; macSÞ; with id a randomly generated route identifier, sn a session number, and macS an MAC on ðrreq; S; T; id; snÞ computed by S using a key shared with T. If S;X1; . . .;Xp; T is a discovered route, then the route reply of the target T has the following fixed form for all intermediate nodesXj, 1 _ j _ p: msgS;T;rrep ¼ ðrrep; S; T; id; sn;X1; . . .;Xp; macT Þ;

where macT is an MAC computed by T with the key shared with S on the message fields preceding it.

B. Ariadne:

Ariadne [19] is an on-demand routing algorithm based on the Dynamic Source Routing (DSR) protocol [2]. There are several variants of Ariadne, depending on which mode of authentication is used to protect route requests: one uses digital signatures, one TESLA [20], and one uses MACs. The MAC version has an optimized variant that uses iterated MAC computations instead of several independent MACs. In addition to being more efficient, the iterated MAC version has superior security characteristics when compared to the nonoptimized version, as noted in [15]. We describe this version below. A typical route request that reaches an intermediate node Xj, 1 _ j _ p, on the route S ¼ X0;X1; . . .;Xp, Xpþ1 ¼ T is of the form msgS;T;rreq ¼ ðrreq; S; T; id;X1; . . .;Xj; macSX1___Xj Þ; where macSX1___Xj is the MAC computed by Xj with a key it shares with T on the route request received from Xj_1: ðrreq; S; T; id;X1; . . .;Xj; macSX1___Xj_1 Þ: The target T, on receiving the last request from Xp, is able to recompute all intermediate MAC values, since it shares a key with each one of the intermediate nodes, and then iteratively reconstruct that sequence up to the last value that should match the MAC received from Xp. If the verification succeeds, with erwhelming probability (given by the security of the MAC construction) all intermediate MACs were correctly computed by the nodes included in the route. The route reply of T is msgS;T;rrep ¼ ðrrep; S; T; id;X1; . . .;Xp; macT Þ; where macT is an MAC computed by T with a key shared with S on the message field that precedes it: rrep; S; T; id;X1; . . .;XpÞ. This is unicast upstream to S via the nodes Xp;Xp_1; . . . , X1. Intermediate nodes must check that their label appears on the route adjacent to two of their neighbors.

III. ANALYSIS OF ARIADNE

A security framework tailored to analyze on-demand source routing algorithms for MANETs. This framework was used to analyze SRP and Ariadne, finding them insecure against hidden-channel attacks, and led to the design of endairA, an on-demand route discovery protocol that the authors claim to be provably secure. Later, _ Acs et al. refined the security framework, A proof of the security claim for endairA is also given in [15]. In this section, the attending attack on Ariadne. We then describe endairA. This discussion is not original and closely parallels arguments in [15]. However, it is directly cogent to the novel arguments that follow (Section 4), which show that the security proof for endairA provided in [15] is flawed, and moreover, this route discovery protocol is not secure even in the (somewhat restricted a plausible route if it can be partitioned into successive subsequences such that 1) the identifiers of each partition are assigned to a single node vi 2 V and 2) the sequence of nodes vi assigned to the partitions forms a simple path in G. This definition is intended to capture the

A. The Security Frame Work Model:

The security framework used by _Acs et al. [15] is based on the simulation paradigm for protocol security, which was envisioned early by Beaver [21] and Beaver and Haber [22] in the context of information-theoretic security. That culminated in two standing (and related) approaches in the (standard) complexity-theoretic security model, developed independently as the secure reactive systems approach by Pfitzmann and Waidner [17] and Backes and Waidner [23] and as the universally composable security fame work by Canetti [18]. These approaches compare executions of a protocol _ in a real-world model to its executions in an ideal-world model that is controlled by the functionality F_, which captures formally the goals that _ is supposed to achieve. In the real world, the adversary is modeled as a traditional Byzantine adversary of the Dolev-Yao model [24], i.e., it is able to schedule and tamper with all communication channels to provide inputs to honest parties and observe their outputs,1 and coordinate the actions of all corrupted parties. Additionally, the adversary is capable of interacting with other sessions of the protocol that may be executing concurrently.2 the ideal-world adversary mimics the behavior of the real-world one to allow for simulations of real-world protocol executions in the ideal world. In order that _ be secure in this framework, the effects on the execution of _ in the real-world model by any real-world adversary A should be indistinguishable from those of an appropriately chosen ideal-world adversary A0 in the ideal world model. In the model described in [15], an MANET is represented by a graph G (V; E), with node set V and edge set E. Each node v is assigned an identifier ‘2 L. It is assumed that the identifiers are authenticated during a neighbor discovery process

B. The Attack on Ariadne:

We briefly describe the attack against Ariadne described in [15]. Consider an instance with source node S and let be a sequence of identifiers of pair wise neighbor nodes inwhich only X; Y are faulty. Let C 6¼ B be another neighbor of both X and Y . In the attack, when the first adversarial node X receives the route request msgS;T;rreq ¼ (rreq; S; T; id; A; macSAÞ; it broadcasts msgS;T;rreq ¼ rreq; S; T; id; A;X; macSAXÞ: This is received by both B and C, which broadcast the corresponding route request. The second adversarial node Y does not respond to either request, while a little later, the first adversarial node X creates a fake route reply in the name of Y : msgS;T;rrep ¼ ðrrep; S; T; id; A;X; B; Y ; macSAXÞ ð1Þ (with the wrong MAC) and unicasts it to B, which only checks the id and that X; Y are its neighbors. Since B has processed an earlier request with identifier id, it will retransmit this, intending it for X. Node Y intercepts it and generates the route request: msgS;T;rreq ¼ rreq; S; T; id; A;X; Y ; macSAXY Þ: This is accepted by D and continued along to T. Since the iterated MAC is correctly constructed, it will be accepted by the target T, which creates and sends back the route reply: msgS;T;rrep ¼ rrep; S; T; id; A;X; Y ; D; macT Þ:

When this reaches Y , the label for node C is added to the listing so that C will rebroadcast it. When X gets it, this label is discarded and the message is sent back to the source S, where it will get validated. In this attack, the adversarial node X ha succeeded in shortening an existing route by using a hidden channel—namely the one provided by the lack of directionality in wireless broadcast—linking it to the second faulty node Y and sending via this channel the message (1) to Y . This message contains macSAX, an MAC that Y needs in order to compute macSAXY . There are several other hidden channels that X and Y could use, as we shall see later

C. The Protocol endairA:

Security and identify a flaw. The proof in [15] considers the possibility of an attack against endairA being successful,hoping to achieve a contradiction.Let ð‘ini; ‘1; . . . ; ‘p; ‘tarÞ be some route that is accepted by endairA, where ‘ini is the label of a nonadversarial initiator node and ‘tar is the label of the target. This is assumed (by contradiction) not to correspond to a valid route in the sense that it includes non-neighbor vertices. Since adversarial nodes can share labels, any number of adversarial nodes can be subsumed in a single label. However, routes (which may appear shorter than actual network routes by collusion of adjacent adversarial nodes) by subsuming all adjacent adversarial nodes, and indeed, any two adversarial nodes with direct means of communication (e.g., via out-of-band channels) as single nodes—see Section 3.1 or [15]. Consequently, adversarial nodes are, by definition, model.

This is an arbitrary restriction that greatly limits the scope of the security statements in the model in their ability to capture realistic security requirements. However, we do not need to leave this model to identify a problem with the security proof of endairA. So, for the sake of argument, we also assume that adversarial nodes are never adjacent. This implies that the route can be uniquely partitioned as follows: each partition consists of a single noncompromised Identifier (label) or a sequence of consecutive compromisedidentifiers. A plausible route is one whose partitions correspond to that of a real route that physically exists in the network. The security statement of endairA is that it only accepts plausible routes. Note that this statement also does not consider an adversarial lengthening of a route by assignment of multiple labels to a single compromised network node as an attack. Again, this is a strong restriction on the security guarantees that the ABV model can provide, but we also follow this paradigm because we wish to show that endairA fails in the exact model in [15]. For the sake of seeking a contradiction, the proof in [15] lets P1; P2; . . . ; Pk be a partition of ‘ini; ‘1; . . . ; ‘p; ‘tarÞ, which is a nonplausible route that has been accepted by endairA. This implies one of the two cases: 1) there exist two

IV. ANALYSIS OF ENDAIRA

The protocol endairA is claimed to be proven secure in the security framework [15]. We now revisit the proof of security and identify a flaw. The proof in [15] considers the possibility of an attack against endairA being successful, hoping to achieve a ntradiction.Let ð‘ini; ‘1; . . . ; ‘p; ‘tarÞ be some route that is accepted by endairA, where ‘ini is the label of a nonadversarial initiator node and ‘tar is the label of the target. This is assumed (by contradiction) not to correspond to a valid route in the sense that it includes non-neighbor vertices. Since adversarial nodes can share labels, any number of adversarial nodes can be subsumed in a single label. However, exclude such faulty routes (which may appear shorter than actual network routes by collusion of adjacent adversarial nodes) by subsuming all adjacent adversarial nodes, and indeed, any two adversarial nodes with direct means of communication (e.g., via out-of-band channels) as single nodes—see Section 3.1 or [15]. Consequently, adversarial nodes are, by definition, never adjacent in model. This is an arbitrary restriction that greatly limits the scope of the security statements in the model in their ability to capture realistic security requirements. However, we do not need to leave this model to identify a problem with the security proof of endairA. So, for the sake of argument, we also assume that adversarial nodes are never adjacent. This implies that the route can be uniquely partitioned as follows: each partition consists of a single noncompromised identifier (label) or a sequence of consecutive compromised identifiers. A plausible route is one whose partitions correspond to that of a real route that physically exists in the network.

The security statement of endairA is that it only accepts plausible routes. Note that this statement also does not consider an adversarial lengthening of a route by assignment of multiple labels to a single compromised network node as an attack. Again, this is a strong restriction on the security guarantees that model can provide, but we also follow this paradigm because we wish to show that endair a fails in the exact model in [15]. For the sake of seeking a contradiction, the proof in [15] lets P1; P2; . . . ; Pk be a partition of ð‘ini; ‘1; . . . ; ‘p; ‘tarÞ, which is a nonplausible route that has been accepted by endairA. This implies one of the two cases: 1) there exist two partitions Pi ¼ f‘jg and Piþ1 ¼ f‘jþ1g such that both ‘j and ‘jþ1 are identifiers that correspond to nonadversarial nodes that are not neighbors or 2) there exist three partitions Pi ¼ f‘jg, Piþ1 ¼ f‘jþ1; . . . ; ‘jþqg, and Piþ2 ¼ f‘jþqþ1g such that ‘j and ‘jþqþ1 are noncompromised identifiers and ‘jþ1; . . . ; ‘jþq are compromised identifiers, but the nodes corresponding to ‘j and ‘jþqþ1 do not share a common adversarial neighbor. The flaw in the proof is the argument against the possibility of case 2. Quoting: “Machine3 ‘j must have received msg0 ¼ ðrrep; ‘ini; ‘tar; ð‘1; . . . ; ‘pÞ; ðsig‘tar ; sig‘p ; . . . ; sig‘jþ1 Þ from an adversarial neighbor, say, A, since ‘jþ1 is compromised. . . . . .In order to generate msg0, machine A must have received msg00 ¼ ðrrep; ‘ini; ‘tar; ð‘1; . . . ; ‘pÞ; sig‘tar ; sig‘p ; . . . ; sig‘jþqþ1 Þ Because, by assumption, the adversary has not forged the signature of ‘jþqþ1, which is non-compromised. Since A has no adversarial neighbor, it could have received msg00 only from a non-adversarial machine. . . . . ” The fallacy with the above reasoning is contained in the last sentence: there is no such necessity for the adversarial node A to get information from a nonadversarial node. initiated by adversarial nodes (in compliance with an ABV model restriction), they just need to be initiated by honest nodes prompted by the adversary (through route discovery requests). Similarly, the requests do not need to be initiated dynamically makes the unwarranted assumption that no direct channels imply no direct bandwidth between adversarial nodes; the proof is therefore incomplete. It could be possible that the security claims remained valid even as their proof is incorrectly argued.

V. THE UNIVERSAL COMPOSABILITY FRAMEWORK FOR ROUTING ALGORITHMS

It is well known that attacks on ad hoc routing protocols can be very subtle. Attacks may exploit the nature of the wireless medium, the mobility of the system, power constraints, and more generally, the fact that the adversary is not necessarily bounded by the constraints on no-fault nodes (the system). It is important that such issues be taken into account when designing security models for wireless systems, and more generally, models for ubiquitous applications. The universal composability (UC) framework [18] and the secure reactive systems model [17], [23] were designed to deal with the composition of concurrent protocol execution attacks, and are therefore, more appropriate models for ubiquitous applications. Obviously, one has to make allowances for the constraints imposed on ad hoc network systems and for the fact that their mobility may make conventional route discovery infeasible (e.g., when routes become disconnected by the time they are discovered4). Below, we list some important aspects that are often neglected in order to make security issues more manageable. Medium during neighbor discovery at the network layer (e.g., by using radio frequency fingerprinting [29]). In a wormhole attack, the adversary establishes an outof- band channel, or a system channel, to subvert the normal functioning of an ad hoc network. In the context of routing, this attack can be used to corrupt routing protocols (as we did in Section 4). Wormhole attacks can be combined with timing or rushing attacks [30] in which the attacker succeeds in forwarding packets faster by using appropriate mechanisms or channels (possibly out-of-band). As with the Sybil attacks, these attacks are usually discounted as preventable at the network layer.

It should be pointed out that claiming that an attack is easily preventable at the network layer is in many respects equivalent to claiming that the security of a wireless system can be achieved at the physical layer. Although, this may be the case for some restricted applications, yet it fails to take into account the malicious nature of some attacks. Note that route discovery is a distributed (global) computation, whereas neighbor discovery is a local process. Therefore, route discovery is better suited to identification of threats 4. In such cases, one may use one of the adaptive gossip protocols in [27]. 5. This would make them “virtual” neighbors of some nonadversarial nodes, which would be in their broadcast range, but they could only receive messages from these nodes via out-of-band channels. such as the Sybil and wormhole attacks, which only become detectable when global information is collated. 5.3 Composability Issues We argue that composability is an essential requirement for secure routing in MANETs. Indeed, MANETs can distinctly be characterized from fixed-infrastructure networks by the fact that both the control plane (routing messages) and the data plane (proper communication messages) are highly subject to a variety of attacks. It becomes essential to understand how the security requirements of each layer interfere with each other Indeed, interference between security properties at different layers also manifests itself in the fixed-infrastructure setting.

We illustrate this point with a real-world example, the well-known rogue packet attack against SSL, described, for instance, in [31]. In this active attack, a rushing node injects an SSL packet in an existing TCP connection,recomputing the TCP checksums to ensure acceptance of the inserted packet at the transport layer. When the SSL protocol daemon, residing at the session layer,6 receives the SSL packet (TCP payload), it determines that the packet has been tampered with by failing to verify the message authentication code (that the attacker is unable to forge for lacking knowledge of the shared authentication keys).The packet is therefore discarded at the SSL layer. However, since it was already accepted at the TCP layer,and moreover, has arrived earlier than the legitimate packet from the original sender, it will prevent TCP from accepting the latter (legitimate) packet. This is because the TCP daemon has recorded that packet’s sequence number as already received. The SSL session layer fails to recover the missing data, and therefore, SSL+TCP does not provide availability guarantees. In this scheme, TCP provides availability but not integrity. SSL provides integrity but relies on the availability properties of TCP. This reliance proves unfounded, as the availability guarantees of TCP are only provided under the weaker integrity notion corresponding to verifiability of the TCP checksums. Composability fails accordingly. MANET routing security presents very similar problems. Indeed, as has been demonstrated by the designers of the endairA protocol, even the provision of a single property (safety of routing discovery) requires at least a concurrent approach, as illustrated by the attacks on Ariadne [15].

We extend this observation by remarking that special care needs to be taken when assuming properties of lower network layers, especially when such properties are achieved under restrictions. If such restrictions are incompatible with requirements at other layers, a solution may be nominally composable but incomplete because no comprehensive solution is achieved (or achievable) in composition. As an example of such a shortcoming, we reexamine the endairA protocol. In this protocol, safety-type properties (such as integrity) at the MANET control plane are achieved by assuming restricted availability of transmission channels. However, such restrictions may be fundamentally liveness guarantees (such as availability) at the data (user) plane. For instance, an MANET could enforce that other forms of data transmission are interrupted while routing computations are ongoing, realizing the required restriction and supporting safety at the control plane. However, this strategy puts the liveness requirements of the control and data plane in direct conflict. Denial-of-service attacks against data transmission could be initiated by frequent triggering of new routing computations. Limiting the frequency of new routing computations might prevent such attacks at the expense of reducing the network capability to deal with frequent topology changes. To summarize, in contrast with the situation for fixedinfrastructure networks, where infrequency of topology changes can be assumed, and therefore, it may be acceptable to deny data services to destinations during any period where routing information to that destination is being (re)computed; in MANETs, it is not acceptable to assume temporal disjointness of the routing discovery an data communication phases, and security under composability of different protocols is necessary. It is insufficient to consider only the simpler (and yet hard to achieve) requirement of security under concurrent executions of the route discovery protocol.

A. The Adversary:

It is sometimes suggested that adversarial nodes should be bound by the same constraints as nonadversarial nodes, for example, have similar communication capabilities [15]. This may be the case for some applications, but it is not realistic. Although, it may seem reasonable to assume that the resources of adversarial nodes are (polynomially) bounded, allowing for the constraints on ubiquitous applications, it is unreasonable to assume that adversarial nodes cannot use more powerful transmitters than nonadversarial nodes, say transmitters that are 50 percent more powerful than the norm,5 if with such means they can compromise the system. That being said, it is technically possible and may be convenient in some cases to restrict the communication capability of nodes in a simulation-based security model such as the UC framework or reactive systems, as demonstrated by the ABV communication model.

B. The Communication Medium:

There are several rather nasty attacks on MANETs that are hard to prevent. Of these, the Sybil attack [25] and the wormhole attack [28] are possibly the worst. The Sybil attack deals with problems caused by sharing secret identifying keys: although, a nonfaulty node is uniquely identified by its public keys, a faulty node may present itself as one of several nodes. In particular, a faulty node may present itself as several nodes during the neighbor discovery protocol. Unless there is some way of physically detecting the source of an identifying call, it is hard to detect such attacks. The ABV model seeks to do an end-run about Sybil attacks by considering only partitions of plausible routes.However, as seen above, the multiplicity of identifiers can be used as a hidden channel to perform subtler attacks that the ABV model cannot tolerate.

Ultimately, it is important to provide some security against Sybil attacks, possibly using some additional feature of the physical broadcast medium during neighbor discovery at the network layer (e.g., by using radio frequency fingerprinting [29]). In a wormhole attack, the adversary establishes an outof- band channel, or a system channel, to subvert the normal functioning of an ad hoc network. In the context of routing, this attack can be used to corrupt routing protocols (as we did in Section 4). Wormhole attacks can be combined with timing or rushing attacks [30] in which the attacker succeeds in forwarding packets faster by using appropriate mechanisms or channels (possibly out-of-band).

As with the Sybil attacks, these attacks are usually discounted as preventable at the network layer.It should be pointed out that claiming that an attack is easily preventable at the network layer is in many respects equivalent to claiming that the security of a wireless system can be achieved at the physical layer. Although, this may be the case for some restricted applications, yet it fails to take into account the malicious nature of some attacks. Note that route discovery is a distributed (global) computation, whereas neighbor discovery is a local process. Therefore, route discovery is better suited to identification of threats 4.

In such cases, one may use one of the adaptive gossip protocols in [27]. 5. This would make them “virtual” neighbors of some nonadversarial nodes, which would be in their broadcast range, but they could only receive messages from these nodes via out-of-band channels. such as the Sybil and wormhole attacks, which only become detectable when global information is collated.

C. Composability Issues:

We argue that composability is an essential requirement for secure routing in MANETs. Indeed, MANETs can distinctly be characterized from fixed-infrastructure networks by the fact that both the control plane (routing messages) and the data plane (proper communication messages) are highly subject to a variety of attacks. It becomes essential to understand how the security requirements of each layer interfere with each other.Indeed, interference between security properties at different layers also manifests itself in the fixed-infrastructure setting. We illustrate this point with a real-world example, the well-known rogue packet attack against SSL, described, for instance, in [31]. In this active attack, a rushing node injects an SSL packet in an existing TCP connection, recompiling the TCP checksums to ensure acceptance of the inserted packet at the transport layer. When the SSL protocol daemon, residing at the session layer, 6 receives the SSL packet (TCP payload), it determines that the packet has been tampered with by failing to verify the message authentication code (that the attacker is unable to forge for lacking liveness guarantees (such as availability) at the data (user) plane. For instance, an MANET could enforce that other forms of data transmission are interrupted while routing mputations are ongoing, realizing the required restriction and supporting safety at the control plane.

However, this strategy puts the liveness requirements of the control and data plane in direct conflict. Denial-of-service attacks against data transmission could be initiated by frequent triggering of new routing computations. Limiting the frequency of new routing computations might prevent such attacks at the expense of reducing the network capability to deal with frequent topology changes. To summarize, in contrast with the situation for fixedinfrastructure networks, where infrequency of topology changes can be assumed, and therefore, it may be acceptable to deny data services to destinations during any period where routing information to that destination is being (re)computed; in MANETs, it is not acceptable to assume temporal disjointness of the routing discovery and data communication phases, and security under composability of different protocols is necessary. It is insufficient to consider only the simpler (and yet hard to achieve) requirement of security under concurrent executions of the route discovery protocol.

VI. SECURE ROUTE DISCOVERY CHALLENGES

In this section, we remark that it is not possible to achieve secure route discovery in an MANET within a composable security framework that does not incorporate additional global and physical information, if the route sought is a simple path (as in Section 3.1). 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 impossibility of finding secure routes but the impossibility of finding paths that correspond to physical routes in the network. Our argument about the impossibility of secure discovery of routes is simple and has been articulated throughout the paper. We base it on the fact that every route discovery algorithm is, in practice, vulnerable to attacks that exploit alternative communication channels to articulate distributed attacks by “encapsulating” and tunneling routing requests. Therefore, it does not seem possible to capture or “model out” Sybil and wormhole attacks from pure-protocol-based security models. The purpose of routing being to establish a communication infrastructure, it is

© 2010, IJARCS All Rights Reserved

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. In the following, we consider two such approaches: multipath routes and route discovery with traceability. 6.1 Multipaths and Subgraphs Routes need not be restricted to paths in the network 1186 IEEE Transactions on Mobile Computing, vol. 8, no. 9, september 2009 restricted availability of transmission channels

A. Multipaths and Subgraphs:

Routes need not be restricted to paths in the network graphG: Any subgraphGST ofGthat links the source S to the target T can be used for communication. Of particular interest, from a security point of view, are subgraphs GST 6. According to the OSI 7-layer network model, or the application layer according to the 5-layer TCP-IP network model.with multiple connectivity between S; T, for example, multipaths [32]. Such routes may have sufficient redundancy to guarantee communication, i.e., may contain at least one secure path (with no adversarial nodes). Obviously, such routes will have additional communication overhead. However, there are ways to partly mitigate this. For example, the source can select communication paths in GST on a rotation basis (adaptive multipath routing [32]). Another approach is to use random subgraphs GST of G that link S; T. Gossip protocols [27] use this approach, which guarantees packet propagation while minimizing the number of nodes that forward packets. The latter approach completely blurs all separation of the routing discovery, maintenance, and data communication phases. Paradoxically, this approach’s meshing of functionalities may facilitate showing the composability of its security properties.

B. Route Discovery with Traceability:

In general solutions such as those proposed above are only appropriate for applications in which security is critical. Perhaps, a more practical solution would be to use routing algorithms that trace malicious behavior—see, e.g., [33]. 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 [33]). 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.

VII. CONCLUSION

A new security framework tailored for on-demand route discovery protocols in MANETs was proposed in [15]. This represents a first effort toward a formal security model that can deal with concurrent attacks and is successful in mitigating a class of hidden channel attacks—the attacks that are intrinsic to the wireless broadcast medium in a neighborhood. However, as we observed above, there are a plethora of other hidden channels that become available through concurrent execution of route discovery protocols. Additionally, in the context of mobility, which requires that route discovery take place simultaneously with data munication, large additional bandwidth is naturally generated and available to adversarial nodes. Consequently, in the proposed formal model, it is impossible to prevent that adversarial nodes break up routes by inserting nonexisting links. To address this shortcoming, either more flexible definitions of routes must be employed (e.g., redundant routing) or it becomes necessary to address global threats directly, such as those posed by Sybil, wormhole, and more generally, man-in-the-middle attacks.

VIII. KNOWLEDGMENTS

The authors would like to thank Tri van Le for helpful discussions.

IX. REFERENCES

[1]. C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Proc. ACM SIGCOMM, pp. 234-244, 1994.

[2]. D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, eds., Kluwer Academic Publishers, 1996.

[3]. P. Papadimitratos and Z. Haas, “Secure Routing for Mobile Ad Hoc Networks,” Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS ’02), 2002.

[4]. C. Perkins, “Ad-Hoc On-Demand Distance Vector Routing,” Proc. Military Comm. Conf. (MILCOM ’97), panel on ad hoc networks, 1997.

[5]. C.E. Perkins and E.M. Belding-Royer, “Ad-Hoc On-Demand Distance Vector Routing,” Proc. Second Workshop Mobile Computing Systems and Applications (WMCSA ’99), pp. 90-100, 1999.

[6]. M.G. Zapata, “Secure Ad Hoc On-Demand Distance Vector Routing,” Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 106-107, 2002.

[7]. P. Papadimitratos and Z. Haas, “Securing Mobile Ad Hoc Networks,” Handbook of Ad Hoc Wireless Networks, M. Ilyas, ed.,CRC Press, 2002.

[8]. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M.Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks,”Proc. IEEE Int’l Conf. Network Protocols (ICNP ’02), pp. 78-89, 2002.

[9]. Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.

[10]. Y.-C. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks,” Proc. IEEE INFOCOM, 2003.

[11]. Y.-C. Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” IEEE Security and Privacy, vol. 2, no. 3, pp. 28-39, Mar.2004.

[12]. L. Buttya´n and I. Vajda, “Towards Provable Security for Ad Hoc Routing Protocols,” Proc. ACM Workshop Ad Hoc and Sensor Networks (SASN ’04), 2004.

[13]. 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.

[14]. 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.

[15]. 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.

[16]. G. _ Acs, L. Buttya´n, and I. Vajda, "Modelling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks," Proc. Workshop Security in Ad Hoc and Sensor Networks (SASN '06), pp. 49-58, 2006.

[17]. B. Pfitzmann and M. Waidner, "Composition and Integrity Preservation of Secure Reactive Systems," Proc. ACM Conf. Computer and Comm. Security, pp. 245-254, 2000.

[18]. R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," Proc. IEEE Ann. Symp. Foundations of Computer Science (FOCS '01), pp. 136-145, 2001.

[19]. Y.-C. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. ACM MobiCom, 2002.

[20]. J.T.A. Perrig, R. Canetti, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc. IEEE Symp. Security and Privacy, pp. 56-73, 2000.

[21]. D. Beaver, "Foundations of Secure Interactive Computing," Proc.Conf. Advances in Cryptology (CRYPTO '91), pp. 377-391, 1992.

[22]. D. Beaver and S. Haber, "Cryptographic Protocols Provably Secure against Dynamic Adversaries," Proc. Conf. Advances in Cryptology (EUROCRYPT '92), pp. 307-323, 1992.

[23]. B.P.M. Backes and M. Waidner, "A General Composition Theorem for Secure Reactive Systems," Proc. Theory of Cryptography Conf.(TCC '04), pp. 336-354, 2004.

[24]. D. Dolev and A. Yao, "On the Security of Public Key Protocols," IEEE Trans. Information Theory, vol. 29, no. 2, pp. 198-208, Mar. 1983.

[25]. J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to- Peer Systems (IPTPS '02), pp. 252-260, 2002.

[26]. G. Simmons, "The Subliminal Channels of the US Digital Signature Algorithm (DSA)," Proc. Third Symp. State and Progress of Research in Cryptography, pp. 35-54, 1993.

Short Bio Data for the Authors

G. YeduKondalu received his MCA degree in Computer Science in the year 2006 from Kakatiya University, Warangal and also M.Tech in Computer Science from JNTUH in 2009-11. At present working as Assistant Professor in CSE department at Swarana Bharathi Institute of Science and Technology, Khammam, AP, His research interest includes Network Security and MANETs.

M. Srinivas received his M.Sc degree in Computer Science in the year 2001 from Andhra University, Vizag and his M.Tech in PARALLEL COMPUTING in the year 2010 from JNT University, Hyderabad. At present working as Assistant Professor in CSE department at Swarana Bharathi Institute of Science and Technology, Khammam, AP, His research interest includes parallel computing and MANETs..

V. Kondal Rao received his M.Sc degree in Computer Science in the year 2001 from Kakatiya University, Warangal and his M.Tech in Computer Science in the year 2010 from JNT University, Hyderabad. At present working as Assoc. Professor in CSE department at Swarana Bharathi Institute of Science and Technology, Khammam, AP, His research interest includes Network Security and RTOS.

R. Ravikumar received his MCA degree in the year 2001 from Kakatiya University, Warangal and his M.Tech (CSE) from JNT University, Hyderabad in 2008-10. At present working as Assistant Professor in CSE department at Swarana Bharathi Institute of Science and Technology, Khammam, AP, His research interest includes Network Security, Parallel Algorithms and MANETs.