IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727Volume 7, Issue 3 (Nov. - Dec. 2012), PP 09-14
www.iosrjournals.org

Active Source routing protocol in Mobile Network

Anamika Bhushan[1,] Divya Gupta[2,] Anil Kumar[3]
[1,2,3] *B-Tech Final Year, Department of Computer Science and Engineering, Institute of Technology And Management, GIDA, Gorakhpur, India.*

Abstract: *The vision of nomadic computing with its ubiquitous access has stimulated much interest in the Mobile Ad Hoc Networking (MANET) technology. However, its proliferation strongly depends on the availability of security provisions, among other factors. We address the problem of secure and fault-tolerant communication in the presence of adversaries across a multi-hop wireless network with frequently changing topology. To effectively cope with arbitrary malicious disruption of data transmissions, we propose and evaluate the secure message transmission (SMT) protocol and its alternative, the secure single-path (SSP) protocol. Among the salient features of SMT and SSP is their ability to operate solely in an end-to-end manner and without restrictive assumptions on the network trust and security associations. As a result, the protocols are applicable to a wide range of network architectures. We demonstrate that highly reliable communication can be sustained with small delay and small delay variability, even when a substantial portion of the network nodes systematically or intermittently disrupt communication. SMT and SSP robustly detect transmission failures and continuously configure their operation to avoid and tolerate data loss, and to ensure the availability of communication. This is achieved at the expense of moderate transmission and routing overhead, which can be traded off for delay. Overall, the ability of the protocols to mitigate both malicious and benign faults allows fast and reliable data transport even in highly adverse network environments.*

Keywords*-Secure Message Transmission, Multi-path Routing, Secure Routing, Secure Routing Protocol , Fault tolerance, mobile ad hoc network (MANET) security, network security, secure data transmission.*

I. Introduction

The Emerging technology of *mobile ad hoc networking*(MANET) is based on wireless multi-hop architecture without fixed infrastructure and prior configuration of the network nodes. The communication in mobile ad hoc networks comprises two phases, the route discovery and the data transmission. In an adverse environment, both phases are vulnerable to a variety of attacks. First, adversaries can disrupt the route discovery by impersonating the destination, by responding with stale or corrupted routing information, or by disseminating forged control traffic. This way, attackers can obstruct the propagation of legitimate route control traffic and adversely influence the topological knowledge of benign nodes. However, adversaries can also disrupt the data transmission phase and, thus, incur significant data loss by tampering with, fraudulently redirecting, or even dropping data traffic or injecting forged data packets. The salient features of this new networking paradigm include: 1) collaborative support of basic networking functions, such as routing and data transmission; 2) lack of administrative boundaries of the network nodes; 3) absence of a central entity in the network; and 4) transient, in general, associations of the network nodes. As a result, a node cannot make any assumption about the trustworthiness of its peers, which assist the node with its communication and, in general, does not possess their credentials. Securing the basic network operation becomes one of the primary concerns in ad hoc networks and, in fact, a prerequisite for reliable and quality-of-service (QoS) communication in adversarial environments.

The challenge lies in securing communication and maintaining connectivity in the presence of adversaries, across an unknown, frequently changing multi-hop wireless network topology. To address this complex problem and provide comprehensive security, both phases of the communication, the route discovery and the data transmission, must be safeguarded. Recently, a number of works proposed secure routing mechanisms to defend against a range of attacks under different assumptions and system requirements [1]–[8]. However, secure routing protocols alone, which ensure the correctness of the route discovery, cannot guarantee secure and undisrupted delivery of data. In other words, a correct, up-to-date route cannot be considered automatically free of adversaries. An intelligent adversary can, for example, follow the rules of the route discovery, place itself on a route, and later start redirecting traffic, dropping, or forging and injecting data packets. Clearly, an adversary can hide its malicious behavior for a long period of time and strike at the least expected time. Thus, it is impossible to discover such an adversary prior to its attack. MANET routing, as well as secure routing protocols assume mechanisms, such as reliable data link layer and route maintenance, which were not designed for and cannot cope with malicious disruptions of the data transmission. Reliable transport protocols cannot address the problem either: an attacker can forge, for example, transmission control protocol (TCP) acknowledgment, while dropping data packets, misleading two communicating nodes that the data flow

is undisrupted. End-to-end security such as the IP-Security (IPSec) [9] authentication header (AH) protocol [10] can prevent adversaries from forging or corrupting data and feedback. But IPsec does not allow the sender to detect loss of data and, thus, take any corrective action. Nor the combination of security services and reliable transport [e.g., stream control transmission protocol (SCTP) [1]] provides an effective solution: a communication failure can be detected, but the same, structurally intact yet compromised path will be repeatedly utilized, because the transport layer protocol cannot influence the choice of the route in the network. Finally, multipath transmissions [2]–[4], can protect against failures. However, "blind" redundant transmissions alone can be highly inefficient without a robust mechanism to detect transmission failures and adapt to the network loss conditions. Our contribution is a novel, general solution, tailored to the MANET requirements, to effectively and efficiently secure the data transmission phase: the secure message transmission (SMT) and secure single-path (SSP) protocols. We emphasize that the goal of SMT and SSP is not to securely discover routes in the network—they assume that secure discovery of routes has been already performed, although routes may not be free of adversaries.

Then, the goal of SMT and SSP, whose basic ideas we presented in [5] and [1], is to secure the data transmission: SMT and SSP operate without restrictive assumptions on the network trust and security associations, promptly detect and avoid nonoperational or compromised routes, tolerate loss of data and control traffic, and adapt their operation to the network conditions. Their main difference is that SMT utilizes multiple paths simultaneously, in contrast to the single-path operation of SSP. In this paper, we extend, refine, and analyze the operation of the two protocols. We present details and analyses of their mechanisms, including their interaction with the route discovery and the maintenance of multiple paths, the path-rating algorithm and a decision-theoretic model for the selection of its parameters, an algorithm to estimate the probability of path survival, and three alternative algorithms for automatic configuration of multipath transmissions. Last but not least, we evaluate the performance of SMT and SSP in a realistic network, integrating SMT and SSP with the secure routing protocol (SRP) [1], [7] and the IEEE 802.11 [8] as the data link protocol, and investigate the interaction of SMT and TCP. Our experiments show that SMT and SSP can support applications with differing objectives and operate in a wide range of network conditions. The simultaneous usage of multiple paths and the dispersion of transmitted data enable SMT to support real-time traffic or other time-sensitive applications, even in highly adverse environments. We also identify increased network load as a factor that can magnify the impact of attacks by relatively weakening the fault detection mechanisms. We combine SMT with TCP to provide flow control, and investigate their interaction: SMT thwarts malicious and benign faults, while TCP adjusts the end-to-end data rate according to the network conditions. Finally, we find that, with SMT, persistent disruption of the data transmission is more effective, from the adversary's point of view, than intermittent or "low-profile" attacks. Overall, our experiments show that SMT and SSP are versatile, effective, and efficient in a wide range of settings. In the rest of this paper, we give a brief overview of the SMT and SSP, after introducing the network and security models.

II. Existing Work

The sections below survey, analyze, and compare four proposed schemes that aim to improve data security in hostile and dynamic MANET environments, namely SPREAD [2], SMT [8], SDMP [8], and Jigsaw Puzzle [4]. As mentioned previously, these schemes leverage the existence of multiple paths between end-nodes to statistically enhance data confidentiality and data availability. Some of the schemes also present ways to preserve data integrity during message exchange. All of the schemes address data confidentiality, while data integrity and data availability are addressed by only some of the schemes. This focus on data confidentiality exists because of the potentially large susceptibility of wireless communications to eavesdropping attacks. Furthermore, data confidentiality is of prime importance in military communications, which is a major application for these schemes.

III. Literature Syrvey

3.1network And Security Model

We define a network node as a process with: 1) a unique identity V ; 2) a public/private key pair Ev , Dv ; 3) a module implementing the networking protocols, e.g., routing, data transmission; and 4) a module providing communication across a wireless network interface. The combination of an Internet protocol (IP) address and a public key can uniquely identify a node. We assume that any two nodes S and T that wish to communicate in a secure manner are capable to establish an end-to-end security association (SA). Since symmetric-key cryptographic primitives are computationally more efficient than public-key ones, we assume that a symmetric shared keys, $K_{S,T}$ instantiates the SA between the end nodes, the source S and the destination T. $K_{S,T}$ can be established through an authenticated Diffie–Hellman exchange [9] integrated with the initial route discovery [7]. Other methods to bootstrap associations are surveyed in [1].We emphasize that the operation of SMT and SSP does not require that S and T are securely associated with any of the remaining, intermediate

network nodes, which assist the S, T communication. We make no assumptions on the behavior or the motivation of the intermediate nodes; they are either correct, that is, comply with the protocol rules, or adversaries, eviating from the protocol definition in an arbitrary manner. Adversaries can target the route discovery and the data transmission, corrupting, forging, or replaying routing, control, and data packets, mounting an attack either intermittently or persistently, in an attempt to control or deny communication. We define a route as a sequence of nodes $\{V_0,V_1\ldots\ldots\ldots V_n\}$, which we denote as(S,T) -*route* when $S=V_0$ and $T=V_n$. The route discovery can be *explicit*, with the protocol returning the entire sequence of nodes, or *implicit*, with the protocol performing a distributed computation returning a (V_i,V_{i+1},V_n)-tuple of the form (*current node*, *relay node*, *destination*) at each node V_i € (S,T) -route, i=0,1…….n-1. We assume that a secure routing protocol safeguards the route discovery, discarding erroneous connectivity information, and returning correct routes. A secure routing specification, that is, the sought properties for discovered routes, independently of the protocol operation, along with analyses of secure routing protocols [7].

3.2 Secure Data Transmission

The Secure Message Transmission (SMT) scheme addresses data confidentiality, data integrity, and data availability in a highly adverse and mobile MANET environment [8]. The SMT scheme operates on an end-to-end basis, assuming a Security Association (SA) between the source and destination nodes, so no link encryption is needed. This SA between end-nodes is used to provide data integrity and origin authentication, but it could also be utilized to facilitate end-to-end message encryption. The scheme works on top of existing secure routing protocols, which cannot by themselves ensure data security. Much like the SPREAD scheme, SMT uses multipath routing to statistically enhance the confidentiality and availability of exchanged messages between the source and destination nodes. Whereas SPREAD was primarily designed with the confidentiality of data transmission in mind, the designers of SMT focused primarily on the reliability of data transmission. SMT provides an explicit end-to-end secure and robust feedback mechanism that allows for fast reconfiguration of the path-set in case of node failure or compromise. Each path is continually given a reliability rating that is based on the number of successful and unsuccessful transmissions on that path. The SMT scheme proposes the use of an Information Dispersal Algorithm (IDA) [3] to divide messages into multiple pieces, each containing limited redundancy. Each piece is transmitted on a different node-disjoint path. A Message Authentication Code (MAC) is transmitted with each piece to provide data integrity and origin authentication. The information redundancy factor is the ratio N/M where any M out of N transmitted pieces are needed to reconstruct the original message. Note that, unlike the case with threshold secret sharing algorithms, it is not guaranteed that less than M pieces will not reveal any information about the original message. Data redundancy coupled with multipath routing ensures that the destination can reconstruct the original message even if some of the pieces are lost in the network. Thus, retransmissions of lost packets are often eliminated, which potentially allows SMT to support real-time traffic with QoS requirements. The simulation results for SMT show that this scheme can successfully cope with a large number of adversaries in the network. In fact, SMT can successfully deliver more than twice the number of packets that can be delivered by a protocol employing secure route discovery but no secure data forwarding6. In addition, the use of multipath routing enables SMT to deliver data with significantly lower end-to-end delays than schemes employing unipath routing. This difference is amplified as the number of hostile nodes in the network increases. In the presence of adversaries, routing overhead is lower than with unipath schemes, because the use of multiple paths allows for less frequent route discoveries in the case of path failures. However, as with SPREAD, the network bandwidth overhead of SMT is larger than that of unipath routing schemes. Also similar to SPREAD, simulation results show that two node-disjoint paths can be found with high probability.

3.3 Security Protocol For Reliable Data Delivery

The Security Protocol for Reliable Data Delivery (SPREAD) scheme addresses data confidentiality and data availability in a hostile MANET environment [6]. The confidentiality and availability of messages exchanged between the source and destination nodes are statistically enhanced by the use of multipath routing. At the source, messages are split into multiple pieces that are sent out via multiple independent paths1. The destination node then combines the received pieces to reconstruct the original message. The SPREAD scheme assumes link encryption between neighboring nodes, with a different key used for each link.

Thus, to compromise confidentiality of a secret message, an adversary has to collect and decrypt all pieces of the message. Since each piece takes a different independent path, the adversary must be present in multiple physical locations at the same time to overhear or intercept all of the pieces2.The SPREAD scheme proposes the use of a (T,N) Threshold Secret Sharing algorithm [5] to divide messages into multiple pieces. A (T,N) threshold secret sharing algorithm can divide a message into N pieces, called shares, such that the original message can be reconstructed from any T shares, where T <= N, while any number of shares less than T cannot yield any information about the original message. SPREAD uses Threshold Secret Sharing with multipath

routing to achieve optimal data confidentiality, where an adversary must compromise all of the utilized paths to compromise an end-to-end message. To compromise a given path, an adversary must compromise at least one node on that path. Formally, let pj denote the probability that a given path j is compromised and let qi denote the probability that a given node i on path j is compromised. It follows that $pj = 1-(1-q1)(1-q2)\cdots(1-qn)$, where nodes 1, 2, ..., n comprise path j. Assume that a total of M independent paths are utilized to relay an end-to-end message. Optimal data confidentiality is trivially achieved when T = N, and between 1 and T −1 shares are allocated to each utilized path. However, to improve data availability, redundancy should be introduced by choosing T < N. This choice of T ensures that the original message can be reconstructed in the presence of node failures, topological changes, or active attacks as long as no more than N − T shares are lost. It can be shown that allocating between N − T + 1 and T − 1 shares to each path provides optimal data confidentiality when redundancy is introduced. Thus, even if a small number of shares are compromised, the confidentiality of the original message remains intact.

The SPREAD scheme employs a custom algorithm to choose an optimally secure path-set that consists of a maximum number of node-disjoint paths. This is a modified version of Dijkstra's algorithm with a security-oriented edge cost function [1] Specifically, the cost cij of an edge between nodes ni and nj is taken to be $cij = -\log q(1-qi)(1-qj)$, where qx is the probability that node x is compromised. The path-selection algorithm considers the security of each individual path based on the probability that a given node along the path will be compromised. This algorithm uses partial network topology information provided by an existing multipath routing algorithm, such as the Dynamic Source Routing (DSR) protocol [4]. The simulation results for SPREAD show that multiple node-disjoint paths can be found in a MANET with high probability 4. Also, the message-interception probability, for both passive and active attacks, rapidly decreases with an increase in the number of paths used to transmit the message. These results show that the SPREAD scheme is capable of enhancing data confidentiality in a hostile MANET environment. It should be noted that the network bandwidth overhead of multipath message transmission is higher than that of minimum-hop Unipath message transmission. This difference occurs because the multiple node-disjoint paths tend to contain more hops and must potentially relay more header information to transmit a given message.

3.4 Secured Data Based Multipath Routing

The Secured Data Based Multipath Routing (SDMP) scheme mainly addresses data confidentiality in a MANET environment [8]. The SDMP scheme assumes Wired Equivalent Privacy (WEP) link encryption between neighboring nodes, which provides link layer confidentiality and authentication. The confidentiality of exchanged messages between the source and destination nodes is statistically enhanced by the use of multipath routing. SDMP uses an existing multipath routing mechanism, making no assumptions about the node-disjointness of the supplied path-set. SDMP requires at least three paths to be present between the source and destination nodes because one path is dedicated for signaling. The SDMP scheme divides the original message into pieces and gives each piece a unique identifier. Pairs of pieces are XOR-ed together, and each pair is sent along a different path. This message division approach is essentially a non-redundant version of Diversity Coding [5], although redundancy could be easily added to provide data availability. Information regarding the pair combinations is sent on the signaling path to allow message reconstruction at the destination. The SDMP scheme assigns data to each path according to the path cost function in order to minimize the time spent at the destination to reconstruct the original message. Unless the attacker can gain access to all of the transmitted parts, the probability of message reconstruction is low.

That is, to compromise the confidentiality of the original message, the attacker must get within eavesdropping range of the source or destination or simultaneously listen on all the paths used and decrypt the WEP encryption of each transmitted part. However, note that it may be possible to deduce parts of the original message from only a few of the transmitted pieces, especially since one piece of the original message is always sent in its original form on one of the paths. The simulation results for SDMP show that the time to send a large message significantly increases as more paths are used. However, using more paths increases the confidentiality of the message. Thus, there is a trade-off between the latency and security of a given message. It should be noted that the use of a dedicated signaling path simplifies the protocol, but also leads to a significant waste of network resources. That is, a significant amount of overhead is required to discover and maintain an extra path that is used to periodically send small amounts of protocol control information. Furthermore, this signaling path creates a single point of failure in SDMP. If an adversary can compromise or jam this path, the entire scheme will cease useful operation until another signaling path can be established.

IV. Discussion And Future Work

In this work, we showed how the data-forwarding phase can be secured by a protocol that operates solely in an end-to-end manner, without any further assumptions on the network trust and behavior of the adversaries. In fact, SMT can counter any attacker pattern, either persistent or intermittent, by promptly

detecting nonoperational or compromised routes. Moreover, SMT bounds the loss of data incurred by an intelligent adversary that avoids detection through manipulation of the path rating scheme. At the same time, SMT provides robustness to benign network faults as well, whether transient or not. Furthermore, resilience to benign faults, along with malicious ones, is important, since in MANET they may be frequent and in practice indistinguishable from forms of denial of-service attacks. Fault tolerance is dependent on the ability of the protocol to determine and utilize alternative, new routes when it detects nonoperational ones. The multiplicity of routes that are, in general, expected to be available in MANET multi-hop topologies can be clearly beneficial. The availability or timely determination of such redundant routes may be the single most important factor for successful transmission across an adverse network. A rich APS, or many alternative routes, can be available only at the expense of routing overhead. This is generally true for any underlying routing protocol, even though the exact amount and type of routing overhead depends on the employed routing protocol. Increasing the size of the APS will most probably increase the routing overhead, which, in the case of reactive routing protocols, may result from more frequent route requests and additional replies, or, in the case of proactive protocols, more frequent link state updates. However, by trading off higher routing overhead, increased reliability (that is, higher fraction of delivered messages) and lower delays can be achieved. In fact, the number of available diverse routes appears to control the trade-off between the delay, the routing and the transmission overhead, and the fraction of delivered messages. For example, the larger the size of the utilized APS, the more probable the successful reconstruction of the dispersed message will be and, consequently, the fewer the data re-transmissions and, thus, the lower the message delay. The protocol adapts to either reduce the overhead or increase its fault tolerance, by selecting for each message the number of paths, among those available, and the redundancy factor. It starts with selecting an APS of *K* shortest (in terms of hops) paths [2].

Without having the opportunity to "probe" the paths and assuming that initially all nodes are equally probable to be malicious, selecting the shortest paths is equivalent to the selection of the most secure paths. The source maintains an estimate, *pi*, of the probability that each APS path is operational. For each combination of the number of paths, *m*, and the feasible values of *r*, the probability that a transmission is successful is calculated with the estimated values for *pi*–s in hand. The source selects *m* and *r* that yield a probability of successful delivery equal or as close as possible to the required probability of successful message delivery, *PGOAL*, (determined, for example, by the application layer). The reader is referred to [8] for additional discussion and implementation details. An open issue of interest is how to obtain estimates or predictions of the probability that a route will be operational. The complexity of such a task is increased, because of the numerous factors that affect the condition of the utilized routes. Mobility, congestion, transmission impairments, and an arbitrary, possibly intermittent and changing over time attack pattern, have to be taken into consideration. Through its interaction with the network and the feedback it obtains from the trusted destination, each node can gradually 'construct' such estimates. Clearly, the network conditions and characteristics can change over time. More simply, parameters such as the network connectivity, density, or the number of attackers present can differ according to the nodes' neighborhood. In any case, a feasible estimation method would be able only to continuously track15 such changes and to provide rough estimates. A plausible approach to obtain the probabilities of operational routes would be to collect statistics on the lifetimes of all the utilized routes.16 It would be helpful to categorize routes according to attributes such as the length or whether the route includes any additional trusted nodes, other than the destination. Moreover, it would be more meaningful to update such measurements by assigning a lower weight to earlier observations in order to account for the network dynamics. For example, a node could quantize path lifetimes and retain measurements and estimates for a set of intervals. Then, if a newly determined path of length i has been operational for a period t in the [tx,tx+1] interval, the node utilizes he estimate of the probability that such a path will survive for a period t' > t, with t' in the [tx+1,tx+2] interval. The investigation and evaluation of such mechanisms are left as future work. Finally, we note that, despite the use of re-transmissions, SMT does not assume the role of a transport layer protocol - it operates at the network layer to secure the data forwarding and improve significantly the reliability of message delivery. However, SMT provides security and protects from frequent disruptions at the expense of increased traffic at the network, especially when data loss is detected. If there is not enough capacity in the network (at the link and at the network layers) to accommodate both the data flows and the SMT's overhead, the upper layer data rate could be decreased, for example, by the congestion control mechanism of the transport layer protocol.

V. Conclusions

In this paper, we have presented the *SMT* protocol to secure the data forwarding operation for *MANET* routing protocols. Our protocol takes advantage of topological and transmission redundancies and utilizes feedback, exchanged only between the two communicating end-nodes. This way, SMT remains effective even under highly adverse conditions. Moreover, features such as low-cost encoding and validation mechanisms, and partial retransmissions render the scheme efficient. By relying solely on the end-to-end security associations, *SMT* can secure effectively the data transmission without prior knowledge of the network trust model or the

degree of trustworthiness of the intermediate nodes. Our performance evaluation confirms that SMT can naturally complement any protocol that secures the route discovery and can shield the network operation by delivering up to 250% more packets despite the presence of substantial fraction of nodes as attackers. We also confirmed that SMT outperforms SSP, a single-path secure data transmission protocol equipped with the SMT's mechanisms. The end-to-end delays achieved by SMT are up to 94% lower than the delays of SSP. Yet, SMT delivers up to 22% more messages. And it does so with 68% lower routing overhead and only with up to 48% data and feedback transmission overhead. In conclusion, SMT's low overhead and its efficient and effective operation render SMT applicable to a wide range of MANET instances.

References

[1] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," in Proceedings of the *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio, TX, Jan. 27-31, 2002.

[2] P. Papadimitratos, Z.J. Haas, and P. Samar, "The Secure Routing Protocol (*SRP*) for Ad Hoc Networks," *Internet Draft, draft-papadimitratos-secure-routing-protocol-00.txt*, Dec. 2002.

[3] M.O. Rabin, "Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance," *Journal of ACM*, Vol. 36, No. 2, pp. 335-348, Apr. 1989.

[4] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed- Hashing for Message Authentication," *RFC 2104*, Feb. 1997.

[5] P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in Proceedings of the *IEEE CS Workshop on Security and Assurance in Ad hoc Networks*, in conjunction with the *2003 International Symposium on Applications and the Internet*, Orlando, FL, Jan. 2003.

[6] A. Tsirigos and Z.J. Haas, "Multipath Routing in the Presence of Frequent Topological Changes," *IEEE Comm. Magazine*, pp. 132-138, Nov. 2001.

[7] J. Broch, D.A. Maltz, D.B. Johnson, Y-C. Hu, J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," in proceedings of the *4th International Conference on Mobile Computing (Mobicom'98)*, 1998.

[8] "Secure on-demand distance-vector routing in ad hoc networks," in *Proc. 2005 IEEE Sarnoff Symp.*, Princeton, NJ, Apr. 2005, pp. 168–171.

[9] S. Kent and R. Atkinson, "Security architecture for the Internet protocol," IETF, RFC 2401, Nov. 1998.

[10] "IP authentication header," IETF, RFC 2402, Nov. 1998.