A metric of trust in Mobile Ad hoc Networks using Direct Source Routing Algorithms

Ralf C. Staudemeyer
University of Applied Sciences Schmalkalden
34 PUBLICATIONS **414** CITATIONS
SEE PROFILE

Christian Omlin
University of South Africa
30 PUBLICATIONS **973** CITATIONS
SEE PROFILE

A Metric of Trust for Ad-hoc Networks using Direct Source Routing Algorithms

D Umuhoza[1,2], RC Staudemeyer[1,2] and CW Omlin[2,3]

[1] Department of Computer Science, University of the Western Cape, Private Bag X17, 7535 Bellville, South Africa
[2] Center of Excellence for IP and Internet Computing, 7535 Bellville, South Africa
[3] Department of Mathematics & Computing Science, University of the South Pacific, Suva, FIJI ISLANDS

Abstract. Security issues and concerns for mobile ad-hoc networks have not yet been satisfactorily addressed, let alone solved. New mechanisms have to be designed and implemented in order to secure communications. In this paper, we present our work in progress on the development of a metric of trust for mobile ad-hoc networks. We introduce the routing problem in mobile ad-hoc networks and present our novel solution which has a number of important advantages over existing solutions.

We give a detailed discussion of this new metric. The traffic analysis technique we use collects information on patterns of communications and performs a statistical analysis on these traffic patterns. The metric is designed to distinguish between malicious security attacks and benign link faults. It is particularly useful in unobservable networks where nodes do not reveal any valuable information and an attacker is forced to launch active attacks.

1 Introduction

Nodes in mobile ad-hoc networks operate in a multi-hop environment. Wireless links are accessible by both legitimate users as well as attackers with malicious intent. Characteristics of mobile ad-hoc networks make the routing process more complex when compared to networks with fixed infrastructure. It becomes even more complex when nodes participating are behaving maliciously.

Two main security issues are detection and protection/prevention of attacks. There is no clear line of defense against security attacks in such networks because of lack of central administration.

We can distinguish between *passive* and *active* attacks. A passive attacker is only able to eavesdrop on the communication medium and observe the traffic flow. It is very difficult to prevent passive attacks since they require an unobservable communication system. A secure system must ensure that an eavesdropper is not able to derive any useful information from watching the communication traffic. Most types of active attacks can be detected because they actively change the state of a network; it is thus possible to deploy defense mechanisms in order to protect a network from active attacks. The question arises how a node or a set of nodes can detect an active attack in progress. Anomalies on a communication link may occur either because of an attack or because of a benign link failure between some intermediate nodes. Any defense mechanism against active attacks must thus be able to distinguish between these two possible sources of anomalous traffic patterns.

In ad-hoc networks, each node simultaneously acts as a router and as a host. The lack of a trustworthy infrastructure requires each node to adopt defense mechanisms and countermeasures against security breaches. Data encryption algorithms can be used to protect the routed information; however, routing information used to propagate IP packets through a network must be accessible to intermediate nodes and this information can be exploited by an intermediate node with malicious intent. While such malicious action cannot be prevented, it can be detected and the thus compromised route can be avoided for all future communication between any two parties.

Trust is a very important concept for security. A node entering a network does not have a priori knowledge of the network or any participating nodes. Thus, nodes must have mechanisms in place to protect their communication.

Our work proposes a metric for measuring the trustworthiness of a communication link between end users in a mobile ad-hoc network. It collects information about communication patterns at the network layer of the TCP/IP-Protocol Stack. The sender and the receiver will record the time stamps of each packet sent and received, respectively. At regular time intervals, the communicating parties will exchange this information. We will derive a statistical model to measure the trustworthiness of a communication link from those observed traffic patterns. These untrustworthy link will then simply be excluded from future communication and communicating nodes will have to find alternative routes. This metric will be applicable to networks that do not disclose any valuable information to an passive observer.

The rest of this paper is organized as follows: In Section 2, we provide brief background information on mobile ad-hoc networks in general and we explain the two major routing protocols in mobile ad-hoc networks: dynamic source routing and ad-hoc on demand distance vector. An overview of routing protocols that incorporate security mechanism follows in Section 3. We state our assumption about the characteristics of networks and describe in detail our metric of trustworthiness in Section 4. We conclude with a summary and direction for future work.

2 Routing in Mobile Ad-Hoc Networks

A mobile ad-hoc network is a collection of self-organized mobile nodes that form a temporary network. Neither pre-defined network infrastructure nor centralized network administration exist. Mobile nodes communicate with each other via radio links; since they have a limited transmission range, nodes wishing to communicate employ a multi-hop strategy for communicating with other mobile nodes.We note that bandwidth available between communicating mobile nodes is restricted since mobile networks have a significantly lower data transmission capacity compared to fixed-line data networks. Furthermore, mobile nodes only have a limited power supply available as power supplied by batteries is easily exhausted. Lastly, mobile nodes may join or leave a network at any given time and frequently change their location in a network; this results in a highly dynamic network topology.

As is the case for infrastructure based networks, the basic problem of routing is to find the lowest cost path between any two communicating nodes. The solution to that problem is to run routing protocols among a subset of intermediate nodes. Classical routing protocol such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) used in fixed-line networks are not suitable for mobile ad-hoc networks. Thus, special routing protocols have been developed to adapt to characteristics of mobile ad-hoc networks. Next we disuss two prominent routing protocols for mobile network that form part of the IETF standard.

Dynamic Source Routing (DSR) is an on-demand protocol, i.e. the route from sender to receiver is only discovered at the time when the sender is ready to send a packet. DSR uses a broadcast technique to discover routes from sources to the destinations as follows: The sender broadcasts a route request message and many such request messages will reach their intended destination. Upon receipt of a request message, the intended recipient node sends a reply message; it follows the reverse path from that of the request message. The originating node in turn receives many reply messages and selects the best route from many possible communication routes.The selected route is kept in the cache for future use.

when a link failures at any intermediate node occurs, an error message is sent to all nodes that use that route for sending their packets and that failing route is removed from the cache. When no alternative routes are available anymore, the route discovery process is restarted [1].

Ad-hoc on demand distance vector (AODV) also is an on-demand protocol and uses the broadcast technique for route discovery. Instead of keeping a table of all possible routes to a destination, a node keeps the address of the next intermediate node on the route to a packet's final destination only. [2].

The above two protocols differ in some important aspects: DSR uses source routing, i.e. it keeps a record of all intermediate nodes of routes to a destination node. Furthermore, it keeps at hand additional alternative routes to be used in case of transport problems along primary routes; thus, if a route fails, an alternative route can be used. AODV, contrariwise, uses table driven routing technique: for each route, each node keeps a record of the next intermediate node only. If a link fails, the route discovery process must be reactivated in order to find an alternative route to a destination node. DSR routes all packets from a source to a destination node along the same route unless a link failure occurs whereas AODV may route packets between the same pair of sender/recipient nodes along different routes. In practice, this means that DSR routing is more like to deliver packets in the order in which they were sent than packets routed by AODV.

3 Related Work

Work in recent years has focused on security aspects of mobile ad-hoc networks. Solutions that extend DSR and AODV routing have been proposed; they address security concerns which previous solutions did not adequately address.
Security Aware ad-hoc Routing (SAR) allows applications to incorporate explicit trust levels into the route discovery process. Users are grouped into different trust levels [3].If one or more users of the same trust level group are compromised, it would expose all users of the same group to securitty attack. In CONFIDANT (Cooperation of Nodes/Fairness in Dynamic Ad-hoc Networks) nodes observe their neigboring nodes as they forward packets to them and update their reputation according to the behavior detected. An alarm message is sent to all other participating nodes in a network whenever a malicious node is detected[4]. Nodes giving false report about their neighbors can force other nodes to be excluded from the network. As nodes will watch their neighbors forwarding packets and report to other nodes in the network, it can facilitate a malicious node that want to identify a certain communication.
Secure Routing Protocol (SRP) guarantees that a node initiating a route discovery will be able to identify and discard any information received from other nodes in a network that provides false topological information [5]. Authenticated Routing for ad-hoc Network (ARAN) proposes authentication, message integrity, and non-repudiation to an ad-hoc environment as a part of a minimal security policy [6]. In Trusted ad-hoc On demand Distance Vector (TAODV) routing, nodes cooperate to obtain an objective opinion about other nodes' trustworthiness. Nodes can thus flexibly choose whether and how to perform data encryption prior to sending packets. Malicious nodes can be detected and excluded from a network [8].
Some of the above protocols secure the route discovery process. Designers of security enhancement algorithms [5],[3],[6]thus must consider the possibility that any node may change its behavior at any time during the communication.[4] and [8] are not considering any distinguish between malicious node behavior and problems caused by traffic congestion or benign link failures which are the most likely causes of routing failures in mobile ad-hoc networks.

4 Metric of Trust

Our metric measures the trustworthiness of a link along the entire communication route based on the observed behavior of traffic patterns. We adjust this trust when traffic patterns change. It will not detect which node is misbehaving among the nodes composing the route, but any two communicating partners will be able to distinguish to some extend between an attacked and a failing link. Our metric does not require nodes to know whether or not their neighboring nodes are forwarding packets. Hence, it will be most useful in unobservable networks where node activities are not supposed to be noticeable and thus cannot be used by an attacker.

There is no way an anomaly in the routing process can be detected if nodes cannot predict the characteristics of the normal routing process. Presently, we are focusing our attention on the timing characteristics of the routing process. A node that initiated a route collects information about packets sent and received, performs a statistical analysis on these patterns and derives a conclusion about the trustworthiness of a route. From this analysis, a node is only able to draw conclusions about attacks initiated by participating nodes i.e. internal attacks; a node may either be compromised or a legitimate user is acting in a malicious manner.

Our metric is able to detect active attacks which in which the attacker intentionally influences the timing of packets so as to be able to identify a communication. These might be by marking single packets ($n = 1$) or by marking the stream of packets ($n > 1$). We distinguish the following types of attacks:

1. delete attack:
   An attacker might delete n packets.
2. delay attack:
   This attack occurs when n packets are maliciously delayed.
3. insertion attack:
   The attacker might insert n packets. These packets might be
   (a) replayed packets or
   (b) new packets.

Our metric of trust works with source routing protocols such as DSR where the initiator of a route keeps a record of the all intermediate nodes all the way to a destination node. The metric is based on the premise that all packets arrive at their destination in the order in which they were sent since they all travel along the same route.

4.1 Premises

We make a number of important assumptions about the characteristics about mobile ad-hoc networks:

1. Encryption and authentication algorithms are implemented for secure data transmission.
2. Although mobile nodes have limited battery life time, they have enough memory to keep and maintain the routing tables and information about traffic patterns.
3. Nodes in a network may move without prior notice but the movement will be moderate.
4. Proper synchronization of the system time between communicating nodes; this is essential for reliable record keeping about packet transmissions.
5. Eavesdroppers cannot derive valuable information from network observations.

Trustworthiness of the link will be measured in three steps: traffic pattern collection, anomaly detection and trust update.

4.2 Traffic pattern collection

The sender initiates the route discovery process by sending the route request message. The intended recipient sends back a route reply message; this establishes the communication link between sender and receiver. Although such communication links are bidirectional, we limit our discussion to unidirectional communication for the sake of simplicity.
The sender keeps a table where an identification number and a time stamp of each sent packet are recorded. The receiver also keeps a table in which an identification number and a time stamp of each received packet are recorded.

4.3 Anomaly detection

After a specific time the receiver sends its table to the sender. The sender merges the two tables into one table containing a packet identifier, a sending timestamp and receiving timestamp for each packet. Using this information the sender can calculate the following values:

- Latency variation of packets
- Change of packets frequency
- Lost packets (packets sent but not received)
- Inserted packets (packets received but not sent)
- Doubled packets (replayed packets)
- Reordered packets

The latency of each packet is calculated using the sender's and recipient's timestamps. The latency of one packet alone is not meaningful but observing the variances and size of latencies can give useful information on detection of attacks.
The change of the packet frequency can be calculated by comparing the sending frequency pattern with the receiving frequency pattern. If there is a time sent entry for a packet but no corresponding time received entry, then that packet was lost. A packet with a time received but no corresponding time sent was inserted by an intermediate node and will also be noted. Multiple time received entries for one packet indicate a replayed packet and will be noted as a doubled packet. Finally, packets that arrive in an order different from the order in which they were sent will be flagged as reordered packets.
Here we give an example of a scenario in practice how the traffic patterns would be collected and anomalies detected. Let's say Alice is communicating with Bob using mobile devices and they are connecting to each other through Claire's mobile device. Alice and Bob keep record of their communication patterns (Time stamp and packet ID) Alice¡————¿Claire¡————¿Bob (sender) (Receiver)

Time Action

150.029611515 Alice sends a packet with ID1 150.02611516 Alice sends a packet with ID2 150.039729243 Alice sends a packet with ID3 150.049947546 Alice sends a packet with ID4 150.060085849 Alice sends a packet with ID5 Bob receives a packet with ID1

150.062083576 Bob receives a packet with ID3 Alice sends a packet with ID6 150.064121879 Bob receives a packet with ID4 150.06932564 Bob receives a packet with ID4

150.074399607 Bob receives a packet with ID2 150.076437334 Bob receives a packet with ID5 150.086495061 Bob receives a packet with ID6

TableI: Traffic patterns collection

After every 0.05ms Bob sends its records to Alice and Alice performs the anomaly detection as described earlier.

Packet Time sent Time Received Latency ID1 150.029611515 150.060085849 0.03047433 ID2 150.02611516 150.074399607 0.044788091 ID3 150.039729243 150.062083576 0.022354333 ID4 150.049947546 150.064121879 0.014174333 150.06932564

ID5 150.060085849 150.076437334 0.016351485 ID6 150.062083576 150.086495061 0.024411485 TableII: Anomaly detection

From the tableI, Alice deduce that packet ID4 was replayed and she also deduces that packet ID2 was delayed and came out of order. The latency of packet is measured in comparison of the minimum latency during the 0.05ms. Those anomalies might have been caused by security attacks or benign link faults , therefore Alice has to update the trust value as it will be described in the following sections.

4.4 Trust update

We will develop a model of trust from a statistical analysis of benign network traffic patterns as follows:

1. We will collect the statistics from normal network traffic.
2. We will introduce faults in the network such as temporarily disabled nodes, link interferences, congestions at intermediate nodes and delays in packet propagation at intermediate nodes; we will record statistics of traffic patterns including distributions of latency and packet losses.

The traffic patterns in the above two cases will be used to characterize normal network behavior. These characteristics of the network will serve to define the threshold value to distinguish security attacks from link failures.
Each time we observe anomalous behavior in the packet flow on the communication link, there is a probability that it is caused by a malicious security attack or by a link fault. We can compute the probability of a security attack occurring and update the trustworthiness of that link accordingly.
There is an initial trust value for a link. It is updated over time based on observed behavior. A link with a negative value of trust will be excluded from all future communication occurring in a network.

4.5 Mathematics model of trust update

Our model is at this stage limited to certain specific cases where certain parameters of the environment can be predictable. For example use of mobile devices in a conference room or in an office or other place where we can predict movement or obstacle between the devices. Therefore it will be possible to calculate the probability of link faults given the parameters. The condition probability and conditional expectation concept is used to carry on the trust modeling. In practice some partial of information is available therefore the desired probability and expectations are conditional ones. Anomalies can be detected as described earlier hence the number of times anomalies occur can be obtained. Anomaly can be the result of two events, attack or link fault. That means, attack and link fault are two independent events that could have resulted into the anomaly. (here comes the formulars....... I still have to finish to write them in Latex)

5 Conclusions

In this paper, we presented our work in progress on developing a metric of trust for mobile ad hoc networks. We discussed how the characteristics of these networks contribute to the routing problem. We gave a brief review of existing solutions to that problem and introduced our novel solution.
We gave a detailed descriptions of our metric of trustworthiness. It is our intention to use traffic analysis techniques to collect statistics of communication pattern under benign as well as suspicious conditions. The metric is intended to distinguish between security attacks and benign link faults. It will be particularly useful in unobservable networks where nodes activities are not supposed to reveal any valuable information to outside observers.
In the next step of our work, we will develop a probability model to implement our metric and we conduct a performance analysis. Security problems in mobile ad hoc networks are not yet fully addressed. More research into novel mechanisms for secure communication in such networks is necessary.

References

1. David B. Johnson, David A. Maltz, and Josh Broch. DSR The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. In Ad Hoc Networking, edited by Charles E. Perkins, chapter 5, pages 139–172. Addison-Wesley. 2001.
2. C. Perkins and E. Royer. Ad Hoc On-Demand Distance Vector Routing. In Proceedings 2nd IEEE Workshop on Mobile Computing Systems and Applications (WM-CSA'99). 1999.
3. S. Yi, P. Naldurg, R. Kravets. A Security-Aware Routing Protocol for Wireless Ad Hoc Networks. ACM Symposium on Mobile Ad Hoc Networking & Computing (Mobihoc '01). October, 2001.
4. S. Buchegger, J.L. Le Boudec, Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks, Proceedings of tenth Euromicro PDP (Parallel, Distributed and Networkbased Processing). January 2002.
5. P. Papadimitrats and Z. J. Haas: Secure Routing Mobile Ad hoc Networks, In Proceedings of the SCS Communication Network and Distributed Systems Modeling and Simulation Conference(CNDS 2002). January 2002.

6. K. Sanzgiri, B. Dahill, B. Neil Levine, C. Shields & E. M. Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks. In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP). November 2002.
7. N. Milanovic, M. Davidson, V. Milutinovic. Routing and Security in Mobile ad hoc Networks, Published in IEEE Computer, Vol. 37, No. 2, p61-65. February 2004.
8. X. Li, M. R. Lyu, and J. Liu, A Trust Model based Routing Protocol for Mobile Ad Hoc Networks, IEEE Aerospace Conference, Big Sky, USA. February 2004.