

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

D. Umuhoza^{1,2}, R. C. Staudemeyer^{1,2}, C.W. Omlin^{2,3}

¹ Department of Computer Science & ² Center of Excellence for IP and Internet Computing, University of the Western Cape, 7535 Bellville, RSA

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 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.

I. INTRODUCTION

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. It should be noted that bandwidth available between communicating mobile nodes is restricted. This is because 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. In mobile ad-hoc networks, nodes operate in a multi-hop environment and each node simultaneously acts as a router and as a host.

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 protocols such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) [1] 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 discuss two prominent routing protocols for mobile network that form part of the IETF standards.

Dynamic Source Routing (DSR) is an on-demand protocol, i.e. the route from source to destination is established when the need arises. 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 route 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 failure at any intermediate node occurs, an error message is sent to all nodes that use that route for sending their packets. The failing route is removed from their cache. When no alternative routes are available anymore, the route discovery process is restarted [2].

Ad-hoc on demand distance vector (AODV) also is an on-demand protocol that uses a broadcast technique for route discovery. When a link failure occurs, an error message is sent to all nodes using that route. The route discovery process is restarted if there is no other route to destination [3].

The above two protocols differ in some important aspects:

- 1) DSR uses source routing technique, i.e. each node keeps in its cache, a record of all alternative routes from source to the final destination. If at some point a link fails, the alternative route is used from source. AODV, contrariwise, uses table driven routing technique. A node only keeps the address of the next intermediate node on the route to a packet's final destination in its routing table. If a link fails, the route discovery process must be reactivated from the point of failure in order to find an alternative route to a destination node.
- 2) 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.

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.

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 path 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 record the time stamps of each packet sent and received, respectively. At regular time intervals, the communicating parties exchange this information. We derive a statistical model to measure the trustworthiness of a communication path from those observed traffic patterns. The untrustworthy path is excluded from future communication and communicating nodes have to find alternative routes. This metric is 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 overview of security enhancements in routing protocols. We state our assumption about the characteristics of networks and describe in detail our metric of trustworthiness in Section 3. We describe how trust is updated after anomaly detection in section 4. We conclude with a summary and give

directions for future work.

II. OVERVIEW OF SECURITY ENHANCEMENTS IN ROUTING PROTOCOLS

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 [4].

In Cooperation of Nodes/Fairness in Dynamic Ad-hoc Networks (CONFIDANT) nodes observe their neighbouring 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 [5].

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 [6]. Authenticated Routing for Ad-hoc Networks (ARAN) proposes authentication, message integrity, and non-repudiation to an ad-hoc environment as a part of a minimal security policy [7]. 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 [9].

Each one of the above protocols has provided a solution to some of the security issues but there are security holes not plugged. Some of the above protocols secure the route discovery process.

- 1) Designers of security enhancement algorithms; SAR, SPR and ARAN thus must consider the possibility that any node may change its behavior at any time during the communication.
- 2) CONFIDANT and TAODV have not considered nor distinguished 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.
- 3) Group security provides an avenue for new attacks and security risks. For example in SAR and in Boukerche et. al. 's novel solution [10] if one or more users of the same trust level group are compromised, it exposes all users of the same group to security attacks.

Nodes giving false report about their neighbors in CONFIDANT 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 wants to identify a certain communication. Our metric considers an environment where only two end nodes collect evidences on the communication. Therefore only two end nodes in a communication are involved

in the process of updating their opinion on the trustworthiness on the communication link. This metric does not consider unchangeable trust among members of a certain group in a network since each node can be individually compromised.

III. METRIC OF TRUST

Our metric measures the trustworthiness of a link along the entire communication route based on the observed traffic patterns. We adjust this trust when traffic patterns change. The intention in this paper is not to localise misbehaving nodes composing the route, but any two communicating partners will be able to distinguish to some extent between an attacked and a failing link. Knowledge of when neighboring nodes are forwarding packets is not required as well. 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, the focus is 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, provided the attacker is participating in the communication process i.e. internal attacks. However, a participating node may have been compromised or a legitimate user is acting in a malicious manner.

Our metric is able to detect active attacks 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 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.

A. Premises

We make a number of important assumptions about the characteristics of 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.

B. 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. Suppose time sent of a packet t_s , time received of the same packet t_r and the packet identification P_{id} . We express traffic pattern T_p as a function:

$$T_p = f(t_s, t_r) + P_{id}$$

C. 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 and keep them in respective variables:

- Trip time variation of packets; Δt_t
- Change of packets frequency; Δp_f
- Lost packets (packets sent but not received); d
- Inserted packets (packets received but not sent); i
- Doubled packets (replayed packets); t
- Reordered packets; r

Trip time t_t of each packet is the time a packet takes from sender to receiver. It is calculated using the sender's and recipient's timestamps.

$$t_t = t_r - t_s$$

The trip time of one packet alone is not meaningful but observing the variances and size of trip times 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

TABLE I
COLLECTION OF TRAFFIC PATTERNS

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

TABLE II
ANOMALY DETECTION

Packet	Time sent	Time received	Trip time
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

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. Having all the variables, we define anomaly as a function of six variables.

$$a = f(\Delta t_t, \Delta p_f, d, i, t, r)$$

In table I and table II we give an example of a scenario in practice how the traffic patterns would be collected and anomalies detected. In this example Alice is communicating with Bob using mobile devices. Since they cannot link directly 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

After every 0.05ms Bob sends its records to Alice. Alice performs the anomaly detection as described earlier. Table I contains the traffic patterns collected during Alice and Bob's communication. It contains the record of actions taken by them and their corresponding time stamps. This table is obtained after Alice merges data collected by herself on her side and data collected by Bob on his side. Table II contains the information Alice have after performing the anomaly detection out of the information contained in table I.

From table I, Alice deduces that packet ID4 was replayed and she also deduces that packet ID2 was delayed and came out of order. The latency of a 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 failure, therefore Alice has to update the trust value as it will be described in the following sections.

IV. TRUST UPDATE

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

- 1) Consider that statistics from normal network traffic exist.
- 2) Faults are introduced in the network such as
 - Temporarily disabled nodes,
 - Link interferences,
 - Congestions at intermediate nodes and
 - Delays in packet propagation at intermediate nodes.
- 3) Records of statistics of traffic patterns are available, including distributions of latency and packet losses.

The traffic patterns in the above mentioned circumstances can be used to characterize normal network behavior. Knowledge of how traffic patterns look like in normal conditions combined with the knowledge how they look like in case of link failure is used to suspect an attacked link. Each time an anomalous behavior on a communication link is observed, there is a probability that it is caused by a malicious security attack or by a link failure. Therefore the probability of security attack occurring and updates of the trustworthiness of that link can be computed.

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 avoided by the communicating partners for that particular communication. Any attacker interested in that particular communication along that path will then not be to perform attack any further.

A. 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, in an office or other place where we can predict movement and obstacle between the devices. Therefore it will be possible to calculate the probability of link failure given the parameters.

When an anomaly occurs the possible cause are i events with probability p_i , $i = 1, 2$.

$$\sum_{i=1}^2 p_i = 1$$

Where p_1 is the probability caused by attack and p_2 is probability of link failure.

The trust update T_u is defined a function of the two probabilities as parameters:

$$T_u = f(p_1, p_2)$$

The knowledge of the parameters of the previous function is used to express the trust update further as an exponential function.

$$T_u = \frac{e^{-p_1}}{e^{-p_2}}$$

As the probability of attack occurring increases the probability of link failure decreases. Consequently the trust value decreases with the increase of probability of attack occurrence.

V. CONCLUSIONS

In this paper, we presented our work 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] Larry L. Peterson and Bruce S. Davie. Computer Networks, A System Approach, Second Edition, p284-292. 2000.
- [2] 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.
- [3] C. Perkins and E. Royer. Ad Hoc On-Demand Distance Vector Routing. In Proceedings 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99). 1999.
- [4] 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.
- [5] 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.
- [6] P. Papadimitratis 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] Boukerche, A., El-Khatib, K., Xu, L., and Korba, L. A Novel Solution for Achieving Anonymity in Wireless Ad-hoc Routing Protocol. Published in the Workshop on Performance Evaluation of Wireless Ad hoc, Sensor and Ubiquitous Networks (ACM PE-WASUN'2004). Venice, Italy. October 2004

