Circle of Trust: One-Hop-Trust-Based Security Paradigm for Resource-Constraint MANET

K. M. Imtiaz-Ud-Din, Touhid Bhuiyan and Shamim Ripon

Abstract Mobile Ad Hoc Networks (MANETs) suffer from acute crisis of resources in terms of battery power, computational ability, and so on. This together with its inherent salient nature makes it very difficult to design effective and efficient security solutions for the MANET. In this kind of dynamic environment, the nodes cannot rely on the conventional measures pertaining to the wired networks. Thus, approaches that depend on trust establishment and evaluation among the nodes are being considered as significant strides toward data protection, secure routing, and other secure network activities. Most of these models can be deemed as rather unscalable due to an excessive exhaustion of resources. In this paper, we limit the region of concern for each node to its one-hop locality and thereby considerably reduce the network overhead. This simple approach to security depending on the principle of mutual trust and prioritization of self-experience has been shown to be effective against a pool of common attacks and feasible with respect to the architectural demand of MANET.

Keywords MANET · Crisis of resource · Trust · Self-experience · Scalability · Introduction

K. M. Imtiaz-Ud-Din (✉) · T. Bhuiyan · S. Ripon
Department of Computer Science and Engineering, East West University, Dhaka, Bangladesh
e-mail: imtu7986@gmail.com

S. Ripon
e-mail: dshr@ewubd.edu

D. P. Mohapatra and S. Patnaik (eds.), *Intelligent Computing, Networking, and Informatics*, Advances in Intelligent Systems and Computing 243,
DOI: 10.1007/978-81-322-1665-0_15,

1 Introduction

The resource-constraint ad hoc networking paradigm relates to a mobile, decentralized and infrastructure less architecture. A set of autonomous nodes or terminals having low computational memory and power resources may form such a network to communicate with each other over a shared wireless channel. These mobile ad hoc networks (MANETs) are dynamic with respect to time as the state of the network may change because of internal movement and external injection or dropout of nodes. This makes the nodes inherently vulnerable to security threats [1]. While the security in ad hoc network is defined as the fixed network by the properties such as availability, integrity, confidentiality, authentication, nonrepudiation, access control, and usage control [2, 3], the methods of defense should not be same. A centralized security solution turns out to be inconsistent with the architecture of the MANET. On the other hand, hierarchical models [4–7] may not be applicable due to reasons such as lack of explicit certificate revocation mechanism, susceptibility to malicious accusation exploits, or the need for an external certificate authority (CA) to revoke the certificates. In addition, the burden of having significantly low resources makes certain method [8] rather invalid and demand for alternate approaches. Trust-based security schemes are proposed in [9–12]. Some of these methods [9, 10] require each node to critically evaluate the trust of every other node in the network and then based on this experience take necessary security measures. This mechanism appears as rather unscalable in an environment where nodes have very limited memory and computational power. Also there is a strong probability that the nodes will fail to pass correct judgment regarding trustworthiness of an increasing number of peers with whom they have had little or no experience of prior communication.

Some other works [13–18] have employed threshold cryptography [19] to build a trust model. This technique manages to overcome the challenges related to certificate administration by distributing the CA duties among n number of network nodes. Any k nodes out of these n nodes will be able to collaborate and act as a single pseudo-CA whereas a coalition of $k-1$ nodes will not be able to fulfill the need. In spite of the seemingly simple solution, threshold cryptography turns out to be a very computationally intensive operation that is not at all suitable for the resource-constraint MANET. Secondly, this approach needs selfless behavior of the peers that is uncharacteristic of the nodes that remain dormant most of the time in order to save battery life.

Other initiatives in this area include clustering-based trust algorithms such as the one proposed in [20]. The authors focus on segmenting the network and emphasize on taking the advantage of a limited domain. Despite this, the model suffers from scalability problem since the node join operation is not bounded by a maximum cluster size. Also, the notion of cluster head acting as a trust guarantor leads to the problem of single point of failure. Denial of service attack (DoS) can be a common threat in this perspective. Finally, the construction of the cluster itself incurs considerable overhead to the networking nodes.

A very different design based on clustering in [21] uses the Web-of-trust model. This suggests a process of calculating trust by considering both direct and recommended trust values. In essence, the method heavily relies on the recommendations from the fellow peers within the same cluster. Thus, a concerted attack by a group of adversaries in which each node certifies every other becomes imminent. The network becomes considerably infiltrated as of the moment a single malicious agent has convinced a user to certify the former. Other more conventional ad hoc network security schemes [22–25] that involve Web-of-trust model also have the same drawback.

In this paper, we present a model that takes into consideration the existing challenges imposed by the architecture of resource-constraint MANET. A single-hop trust scheme is proposed that makes a node consider its neighbor to be trustworthy based on first-hand experience and on accumulated knowledge.

The rest of the paper is organized as follows. Section 2 states the trust model. The next section illustrates the effectiveness of the solution from the security perspective by applying the model to implement a secure routing algorithm. Section 4 analyzes its feasibility in terms of the architecture. Finally, the conclusions and future works are outlined in the last section.

2 The Trust-Based Security Solution

In this section, we focus on characterizing the trust-based security solution. The underlying principle is simple and tries to simulate the rational decision-making process of human beings but on a limited domain. All the interaction among the nodes within the network is dependent on the prior trust analysis and evaluation.

2.1 The Environment

Our environment is a MANET where nodes communicate with one another without any support of physical or logical infrastructure. We also note that majority if not all the devices run on limited resources in terms of memory, battery, and computational power. There may be n mobile nodes where n can vary over time due to the dynamic behavior of node joining, leaving, or movement inside the network. We also make the following assumptions: (1) every node has a mechanism to identify its one-hop neighbors, the maximum number of which is limited by the availability of internal resources (2) each node is able to detect a misbehaving node (if any) in its one-hop neighborhood with certain means such as the ones proposed in [26, 27].

2.2 The Trust Model and the Node Evaluation Scheme

The definition of trust that will be used by us relates to the human trust mechanism. It is the confidence of one node on another based on the expectation that the latter will perform certain actions as entrusted by the former even if the former is unable to influence or monitor the latter [21]. A fuzzy value ranging from 0 to 1 is used to quantify the level of trust. The level of sufficiency of this parameter can vary by a large extent depending on the specific scenario. For example, an application that requires high degree of security will need very trustworthy peers to transmit the data and thus will look for high trust index. The trust index is evaluated based on the following factors each of whose numeric value ranges from 0 to 1 on a continuous scale:

First-hand experience statistics: This is the statistic data of previous experience accumulated while communicating with other nodes. The success of communication through a certain neighboring node will increase its trust index assigned to that node. On the other hand, a failed attempt of data delivery enhances the level of dissatisfaction and therefore will result into decreasing in the index. In addition to this, the level of satisfaction quantified by the delay in data transfer is also taken into account. The function to compute the first-hand experience statistics thus becomes:

$E_{ij} = F_e$ (proportion of successful secured communication of node i through node j, delay in communication)

Intruder nodes: A value of 0 will be assigned to the intruder variable I_{ij} corresponding to node j if j is identified as an intruder by node i. Otherwise, 1 will be assigned.

Other factors: This can include parameters such as frequency of routing request and energy left. Depending on the specific requirement of the particular MANET, management policy, and other constraints, a set of new parameters can also be defined.

$F_{ij} = F_{of}$ (frequency of routing requests from node j to node i, energy left on node i,)

With reference to the above-mentioned factors, the trust index computed by a node i for a node j is given as

$$Ti_{ij} = \left(E_{ij} + I_{ij} + OF_{ij}\right)/3$$

To send some data, the trust index is compared with the current security threshold (ST) which denotes the importance of the data being transferred as well as the level of security of the entire network. While the data value has a directly proportional relationship with ST, the level of security has an inverse impact. This is evident as with a highly secured network, the choice of neighbor becomes more and more irrelevant.

$ST = F_{\mathrm{dv}}$ (importance of data, security level of the network as perceived by node i while sending data to node j)

In addition to comparing the trust index with the *ST*, neighbor selection is also based on another variable called *penalty*. Every node stores this attribute corresponding to each of its neighbor in the trust table (Fig. 1). The higher the number of accusers in the penalty the lower is the trust. A node is penalized by listing its accuser node in the penalty attribute whenever complaints are received against the same from other one-hop neighbors.

2.3 The Architecture

Each node in the network will possess a trust matrix that will incorporate the trust indexes of its one-hop neighbors and their penalty values. We do not feel the necessity of including other nodes as all the communication to and from a certain node is bound to pass through one of its one-hop neighbors. Thus, we define the one-hop community of each node as its circle of trust (CoT). When a node first enters the CoT, its trust matrix is empty. Hence, it requests the trust tables from all of its one-hop neighbor, sets the trust indexes of all peers to 1 (complete trust), and initializes the penalty field corresponding to each peer by retrieving it from their trust tables. If there is a mismatch of any penalty, the newcomer queries the accuser node about the validity of its accusation and eventually identifies the culprit who was misinforming. It then accuses the culprit with charge of intrusion and discards all the penalty values. If a node does not have any penalty value or all the penalty values are equal, it selects a random node for communication. Every node re-computes the trust index of a peer only after a first-hand interaction, and it also unicasts the verdict to the node being judged. Thus, all the peers in the circle are continuously evaluated by one another and the mutual trust values are shared only upon a request from a fellow neighbor. The nodes will not convict a certain node though and degrade its trust value by accusing it as a culprit based on accusations from other nodes. One can only prioritize a node over another node if they have the same trust value and the former has comparatively low penalty against itself.

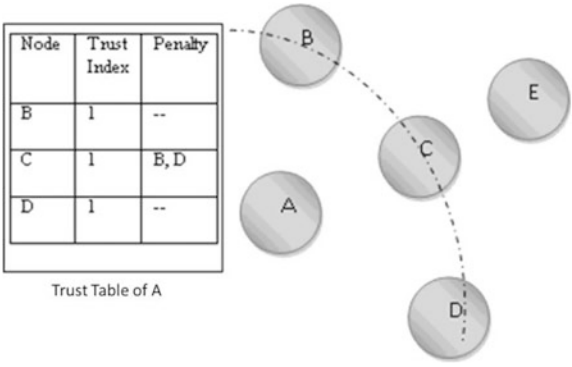

Fig. 1 Circle of trust

A node can accuse its neighbor only once. The accusation is broadcasted when the trust index of the latter has gone below a minimum trust value that is required for any kind of communication with the former. The entries of the accused are then purged from the trust table of the accuser. The only other case when a node can accuse one of its peers is if the former convicts the latter with the charge of intrusion. In both the cases, the network security degradation flag is raised by the accuser and this is noted accordingly by the peers who will then re-evaluate the *ST*.

3 Security Analysis of the Solution

3.1 The Secure Routing Protocol

In this section, a secure source-driven on-demand routing protocol (Fig. 2) is illustrated as a proof of effectiveness of the above trust-based security solution. The protocol assumes the environment to be the one outlined in Sect. 2.1 and builds on the basis of the secure routing protocol as in [9]. It is described as follows:

1. Source node broadcasts route request message to its one-hop peers in order to find a route to the destination.
2. The neighbors of the source forward the request to their neighbors in turn if they find the source to be trustworthy enough to act as an intermediary in the data transfer. The process loops around until and unless the destination node is reached. At this point, a response message is sent upstream along the same path(s) confirming the immediate upstream node(s) about the participation if the downstream node finds its upstream peer/s to be trustworthy enough for any sort of communication. The response message is thus initiated by the destination and forwarded all the way up to the source. At every layer of the CoT, an upstream node selects one of its downstream neighbors as the next hop in the chain and then forwards the response message.
3. When the response reaches the source ROM multiple one-hop neighbors, it picks a neighbor that is most trustworthy and the path that will have the least hop associated to it or that is most secured.
4. The source then sends the data to the destination using the selected route asks for the confirmation of reception and waits for a specified amount of time. If a confirmation is requested, the destination node will send it using the above method but via a different route due to security considerations.
5. If the confirmation is received and is verified as a valid one by the source, it continues to send data using the same route. Otherwise, if the confirmation is not received within the preferred time, the source will update the trust index of its neighboring peer by degrading the corresponding trust value of first-hand experience statistics and will notify the node in question. The same sequence is then iterated by all the nodes, and the degradation of trust propagates along the

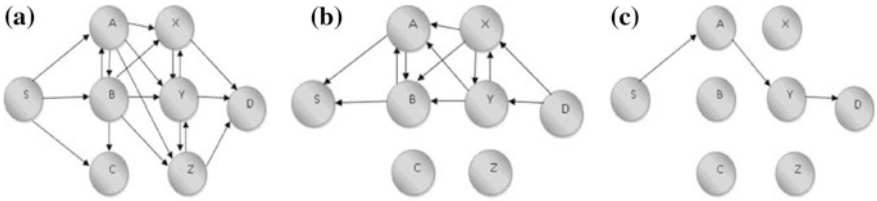

Fig. 2 Trust-based secure routing

entire chain of the route. If at any point a node detects its neighbor as an intruder, it will set the corresponding intrusion value to be 0 and raises the network security degradation flag. The processing then either jumps to 1 for better security or to 6 for better performance.

6. The source selects the next best route.

The protocol outlined above can be implemented by plugging in the trust evaluation scheme into any on-demand ad hoc routing protocol with suitable modifications. With this outlined method, one can achieve security equivalent to maintaining trust information of all the nodes on the path from the source to the destination.

3.2 Analysis Based on Known Attacks

This section highlights the strength of the proposed secure routing protocol by analyzing it over a set of well-known security threats:

Black Hole Attacks: In this kind of attack, an adversary claims itself to be the shortest path to the destination. The sender can eventually detect this kind of malicious activity as it requires the destination to send a delivery confirmation through a different route altogether. If this confirmation does not reach the source within the stipulated time, the following packets are sent across a new route. The mandatory use of a demand route ensures that a fake delivery confirmation generated by the culprit is not accepted by the sender node. Moreover, if the malicious node is detected as an intruder by one of its neighboring nodes, the model ensures that it is deemed as an outcast.

Selfishness: The act of selfishness is heavily penalized in our model. A node that does not route a packet or route request and drops them either with a malicious intent or to save their resources loses its trust to the one-hop sender. The rate of delivery is also considered so that a node that selfishly delays the transmission for long enough time is amerced. A cooperative network is an evident outcome as such.

Denial of Service (*DoS*): The DoS attack is launched by an adversary when it attempts to use up all the network bandwidth and thereby make it unavailable to the other peers. The intrusion detection mechanism that is assumed to be built into

our environment can be used as a remedy to this problem. As for example, if a node generates an excessive amount of route request, the neighbors at one point will start ignoring its request as the frequency of request significantly affects the trust index of the requester. Any of the peers under these circumstances may also broadcast the possibility of intrusion within the CoT. Thus, all the peers can use this warning to revise their trust evaluation matrix and also have a better perspective of their neighborhood in terms of security.

Routing Table Overflow and Energy Consummation: A malicious node can try to initiate routes to nonexistent nodes. The motive is to overwhelm the peers by accumulating enough routes in their routing tables so that creation of new route is prevented. This kind of attack is circumvented by the ability of the peers to reject or ignore the request based on its own resource availability and also the trustworthiness of the requester. This potential of the nodes also help them to survive against adversaries that want to consume all their battery power by forwarding an excessive amount of traffic through them.

Wrong Allegations: Our model successfully fights against the wrong allegations that may be claimed by a malicious node against a well-behaving peer. This is ensured by limiting the number of charges that can be raised by a node against another to just one. Also, this penalty is only considered only if multiple nodes have the same trust index.

4 Discussion

As pointed out in [28], a localized approach to node authentication is the most suitable one according to the architectural requirement of MANET. The proposed model therefore thrives well. Besides eliminating the single point of failure found in some cluster-based designs, limiting the domain of trust to just one-hop neighborhood brings forward some distinct advantages. The information needed to be stored and computed by the nodes goes down to a significantly low range making the design to be absolutely friendly for the resource-constraint nature of the network. This is in contrast to the characteristics of the models, referred in the Introduction section, most of which maintain a network-wide or cluster-wide trust table. In addition to this, the overhead introduced by the trust-based security scheme is also kept to a minimum level by limiting the number of messages exchanged among the nodes. The only time a node shares some information is when a peer requests for the penalty values or it accuses one of its neighbors. All these factors result into a highly scalable system. In addition to this, the self-adaptive nature of the solution makes it rather easy to manage and maintain the security of the network. Although the security level attained during the birth or infancy of the network may be quite ambiguous due to the lack of knowledge among the peers, as time passes, it gradually converges to a stable state where the participants are aware of their individual threats.

Finally, the proposed mechanism has the necessary flexibility as indicated in Sect. 2.2 to resist novel attacks by introducing new parameters into the trust evaluation.

5 Conclusion and Future Work

Ensuring security in resource-constraint MANET presents itself as a complex research challenge. In this paper, we have carefully reviewed the security issues in this kind of network and analyzed the problems related to them. The existing solutions do not take into consideration the limitations imposed by the MANET architecture well. A trust-evaluation-based security paradigm has been proposed in this paper that stresses on personal experience to evaluate the trust of a peer within a very limited domain. This has then been applied to a source initiated on-demand routing protocol that provides equivalent security to maintaining trust information about all the nodes on the path from source to destination. Its security has also been evaluated over a set of major active attacks. The analysis showed that the method fights against these attacks effectively. In addition, we further went on discussing the feasibility of our proposed solution in terms of the architecture and concluded that the network converges to a certain degree of acceptable security as some time elapses and the nodes have accumulated more and more knowledge about one another.

Our immediate future work encompasses analyzing various efficient trust algorithms and formalizing our own trust evaluation method based on the study. We also expect to prove the effectiveness of the proposed model by verifying the solution using a formal model checking tool.

References

1. Biswas, K., Ali, M.L.: Security threats in mobile ad hoc network. M.Sc. Thesis, BTH, Sweden (2007)
2. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Network **13**(6), 24–30 (1999)
3. Zhang, Y., Lee, W.: Intrusion detection in wireless ad-hoc networks. Proceedings of MobiCom 2000, 6th Annual International Conference on Mobile Computing and Networking, Boston, USA, 6–11 Aug 2000
4. Pietro, R.D., Mancini, L.V., Jajodia, S.: Efficient and secure keys management for wireless mobile communications. In: Proceedings of the 2nd ACM International Workshop on Principles of Mobile Computing, pp. 66–73, Oct 2002
5. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., Srivastava, M.: On communication security in wireless ad-hoc sensor networks. In: Proceedings of 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), pp. 139–144, June 2002
6. Cr'epeau, C., Davis, C.R.: A certificate revocation scheme for wireless ad hoc networks. In: Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2003), Oct 2003

7. Housley, R., Polk, W., Ford, W., Solo, D.: Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. Internet Request for Comments (RFC 3280), Apr 2002
8. Davis, C.R.: A Localized Trust Management Scheme for Ad hoc Networks. McGill University, Montreal (2009)
9. Yan, Z., Zhang, P., Virtanen, T.: Trust evaluation based security solution in ad hoc networks. Technical Report, Nokia Research Center, Helsinki, Finland, Oct 2003
10. Pirzada, A.A., McDonald, C.: Establishing trust in pure ad-hoc networks. In: Proceedings of Australasian Computer Science Conference, pp. 47–54, Jan 2004
11. Marsh, S.P.: Formalizing trust as a computational concept. Ph.D. Thesis, Department of Mathematics and Computer Science, University of Stirling (1994)
12. Sarela, M., Hietalahti, M.: Security topics and mobility management in hierarchical ad hoc networks: A literature survey, interim report of project samoyed. Helsinki University of Technology, Apr 2004
13. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Netw. Mag. **13**(6), 24–30 (1999)
14. Kong, J., Zerfos, P., Luo, H., Lu, S., Zhang, L.: Providing robust and ubiquitous security support for mobile ad hoc networks. In: Proceedings of the 9th International Conference on Network Protocols (ICNP), pp. 251–260, Nov 2001
15. Kong, J., Luo, H., Xu, K., Gu, D.L., Gerla, M., Lu, S.: Adaptive security for multi-layer ad-hoc networks. In: Special Issue of Wireless Communications and Mobile Computing. Wiley, Aug 2002
16. Luo, H., Lu, S.: Ubiquitous and robust authentication services for ad hoc wireless networks. In: Proceedings of 7th IEEE Symposium on Computers and Communications (ISCC'02), July 2002
17. Zhou, L., Schneider, F.B., van Renesse, R.: Coca: A secure distributed online certification authority. ACM Trans. Comput. Syst. **20**(4), 329–368 (2002)
18. Luo, H., Zerfos, P., Kong, J., Lu, S., Zhang, L.: Self-securing ad hoc wireless networks. IEEE ISCC 2002
19. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
20. Jin, S., Park, C., Choi, D., Chung, K., Yoon, H.: Cluster-based trust evaluation scheme in an ad hoc network. ETRI J. **27**(4), 465–468 (2005)
21. Ngai, E.C.H., Lyu, M.R.: Trust and clustering-based authentication services in mobile ad hoc networks. In: Proceedings of 24th International Conference on Distributed Computing Systems Workshops—W4: MDC (ICDCSW'04), Hong Kong, China, pp. 582–587 (2004)
22. Capkun, S., Buttyan, L., Hubaux, J.P.: Self-organized public-key management for mobile ad hoc networks. IEEE Trans. Mob. Comput. **2**(1), 52–64 (2003)
23. Capkun, S., Hubaux, J.P., Buttyan, L.: Mobility helps security in ad hoc networks. In: Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003), June 2003
24. Eschenauer, V.D.G.L., Baras, J.: On trust establishment in mobile ad-hoc networks. In: Proceedings of 10th International Workshop of Security Protocols, Springer Lecture Notes in Computer Science (LNCS), Apr 2002
25. Hubaux, J.P., Buttyan, L., Capkun, S.: The quest for security in mobile ad hoc networks. In: Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), pp. 146–155, Oct 2001
26. Zhang, Y., Lee, W.: Intrusion detection in wireless ad hoc networks. ACM MOBICOM (2000)
27. Marti, S., Giuli, T., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. ACM MOBICOM (2000)
28. Yang, H., Zhong, G., Lu S.: Network performance centric security design in MANET. IEEE Mob. Comput. Commun. Rev. **6**, 50 (2002)