A Security Architecture for Tactical Mobile Ad hoc Networks

Hengjun Wang, Yadi Wang, Jihong Han
Zhengzhou Information Science and Technology Institute
Zhengzhou, China
wanghengjun@163.com

***Abstract*—Mobile Ad hoc Network (MANET) is self-organizing, infrastructureless, multi-hop network. The wireless and distributed nature of MANETs and the very bad security environment in battlefield bring a great challenge to securing tactical mobile ad hoc networks. Most schemes proposed recently focus on specific security areas, such as establishing trust infrastructure, securing routing protocols, or intrusion detection and response. Few of the previous work proposes security solutions from a system architectural view. In this paper, we propose security architecture for tactical mobile ad hoc networks, which is layered as network model, trust model and security operations. Three main security technologies applied in this architecture and relationships among them are analyzed in detail.**

Keywords-Mobile Ad hoc network; security; architecture; tactical network

I. INTRODUCTION

Today's warfare is network centric. Communications on the move are essential for successful mission operations. Dismounted tactical soldiers often communicate at short range and peer-to-peer with mobility and task coordination. Mobile Ad hoc networks (MANETs) are self-organizing wireless systems capable of forming networks on the fly, without fixed relays or repeaters. Such a network is highly deployable and exceptionally well suited to handle Lower Tactical Internet communications at brigade and below.

Up to now, some works on securing MANETs have been proposed. But few of them consider designing security mechanisms from a system architectural view. The lack of methodology to manage the complexity of security requirements in variant situations will lead to misplacement of security mechanisms and overlapping of security functionalities.

In this paper, we propose the security architecture based on distributed CA (certificate authority), trust management and secure clustering. It is layered as network model, trust model and security operations from a system viewpoint other than OSI model applied in designing network protocols.

In the following, we first analyze the challenge and goals to the security of MANETs in battlefield. In section 3, the proposed security architecture for tactical MANETs is presented. The main security technologies deal with the architecture and their relationships are introduced and analyzed in section 4. Lastly conclusion is made in section 5.

II. SECURITY CHALLENGES AND GOALS OF TACTICAL MANETS

MANETs are subject to various kinds of attacks due to their nature. Firstly, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering. Wireless communication links can be eavesdropped on without noticeable effort and communication protocols on all layers are vulnerable to specific attacks. In contrast to wire-line networks, known attacks like masquerading, man-in-the-middle, and replaying of messages can easily be carried out. Secondly, deploying security mechanisms is difficult due to inherent properties of MANETs, such as the high dynamics of their topology (due to mobility and joining/leaving devices), limited resources of end systems, or bandwidth-restricted and possibly asymmetrical communication links. Thirdly, mobile devices tend to have limited power consumption and computation capabilities which make it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms. Finally, node mobility enforces frequent networking reconfiguration which creates more chances for attacks, for example, it is difficult to distinguish between stale routing information and faked routing information.

For mission-critical applications such as a military application in a hostile environment there are more stringent security requirements than in MANETs for commercial or personal uses. In tactical MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, in another word, we need to consider both insider attacks and outsider attacks in mobile ad hoc networks, in which insider attacks are more difficult to deal with.

There are five main security services for MANETs [1]. *Authentication* means that correct identity is known to communicating partner; *confidentiality* means certain message information is kept secure from unauthorized party; *integrity* means message is unaltered during the communications; *nonrepudiation* means the origin of a message cannot deny having sent the message; *availability* means the normal service provision in face of all kinds of attacks. Among all the security services, authentication is probably the most complex and important issue in MANETs since it is the bootstrap of the whole security system. Without knowing exactly who you are talking with, it is worthless to protect your data from being read or altered.

978-0-7695-3543-2/09 $25.00 © 2009 IEEE
DOI 10.1109/WKDD.2009.154

III. SECURITY ARCHITECTURE FOR TACTICAL MANETS

Communication between any two nodes in MANETs might require the packets to traverse multiple hops. Several protocols have been proposed in the literature for routing in mobile ad hoc networks [2]. Different with traditional wired networks, the intermediate nodes may be mobile and they can cause frequent link failures and staleness of routes. That in turn can result in route errors and trigger off a fresh route discovery process. So the performance of routing algorithm in MANETs is lower than those in traditional networks. With the increase in size of the networks, flat routing schemes do not scale well in terms of performance and the packets maintaining the routing will exhaust the whole bandwidth. Hence, some hierarchical organization is required in large ad hoc networks, such as encountered in battlefield communications, for solving this problem [3]. Routing on top of clustered topologies is much more scalable than flat routing.

So our security architecture only focuses on large tactical MANETs which are clustered into many small sub-networks. In fact, the flat networks can be seen as only one cluster networks. Conceptual security architecture of the network inspired by [4] is described in Fig. 1. It is layered as network model, trust model and security operations.

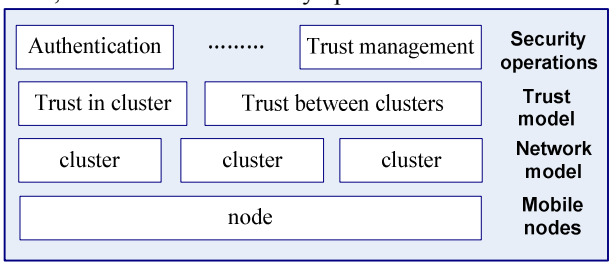

Figure 1. Security architecture for Tactical MANETs

For battlefield communications, trust among nodes is the most important thing. In traditional wired networks, most trust evidences are generated via potentially lengthy assurance processes, distributed offline, assumed to be valid for a long-term and certain at the time when trust relations derived from it are exercised [5]. In contrast, few of these characteristics of trust relations and trust evidences are prevalent in mobile ad hoc networks. Lack of fixed networking infrastructure, high mobility of the nodes, limited range and lack of reliability of the wireless links are some of the characteristics of ad hoc networks that make design of a trust establishment scheme a very difficult and challenging task. In particular, trust relations may have to be established using only online evidence and may be short-term and largely peer-to-peer. Since solutions developed for the fixed wire-line networks are not suitable in such a scenario, some security solutions [6-9] have been proposed for MANETs based on distributed trust model or fully self-organized trust model. Most of the distributed trust models applied in MANETs are based on threshold cryptography. Fully self-organized trust model dose not suit the battlefield for the reason that the building of certificate chain is not efficient enough.

Based on the trust model, many security operations can be carried out. All these operations can be classified as security applications and network security maintenances. Authentication is the first thing for all security applications such as secret communications. Authentication can be easily achieved according to trust model in our security architecture and then confidentiality is a matter of encrypting the session using whatever key material the communicating parties agree on. For reasons that our security architecture combines the network model closely and MANETs are dynamic networks, trust model must be maintained according to network model and trust management though security operations such as trust evidences collecting and trust value evaluation. Node trust evaluation value will not only work on trust model but also network model, for example, the node whose trust value is lower than threshold will be excluded of network.

IV. SECURITY TECHNOLOGIES AND DETAILS OF THE ARCHITECTURE

To cope with all kinds of attacks, our security architecture mainly relies on three security technologies: distributed CA, trust evaluation and secure clustering.

A. Distributed CA.

In traditional wired networks, central servers are available to provide security services for the users inside the network system. In MANETs, absence of fixed infrastructure creates new challenges in security measurements. Up to now, several studies on securing ad hoc networks have been proposed, including key management, key distribution, and secure routing. However, while in ad hoc networks it is difficult to provide on-line access to trusted authorities or centralized servers like CAs, the schemes proposed in these studies usually rely on a CA that is the most important component of PKI and responsible for the validity of digital certificates. Due to the nature of the ad hoc networks, a centralized CA is a network security bottleneck. Multiple replica of CA is fault tolerant, but the network is as vulnerable as single CA or even worse since breaking one of the CAs means breaking all of them. Hence, in order to improve the CA's behavior, the responsibilities of the CA should be distributed among the nodes with highest degree of trustiness. The distributed CA consists of a lot of nodes which provide secure services for themselves and common nodes.

In [10], a key management system based on threshold cryptography has been introduced. A group of n servers together with a master public/private key pair is first deployed by a Certification Authority (CA). Each server has a share of the master private key and only these servers together can form a whole signature. A node that wants to join the network first has to collect all of the n partial signatures but it can obtain the certificate. There are some schemes [10-12] extended or modified from this key management system.

B. Trust evaluation.

Trust is a notion corresponding to a set of relations among entities that participate in various protocols [5]. Trust

relations are determined by rules that evaluate, in a meaningful way, the evidence generated by the previous behavior of an entity within a protocol. In our architecture the evidences are not only the previous behavior within a protocol but also the previous secure services and secure events such as intrusion and being captured. In battlefield, trust relations change frequently because of all kinds of inside and outside attacks.

In previous work done related to intrusion/misbehavior detection and response, the paper [13] proposed two mechanisms: pathrater and watchdog to improve throughput in the presence of nodes that agree to forward packets but fail to do so. Watchdog is used to identify misbehaving nodes while pathrater evaluates node ratings reported by all nodes and gets the result which can be as a path metric to help routing protocols avoid these misbehaving nodes. In [14], MANETs security system is presented based on a "neighborhood watch" concept. Recommended-trust [15] is important for nodes that are not neighbors to decide their behaviors.

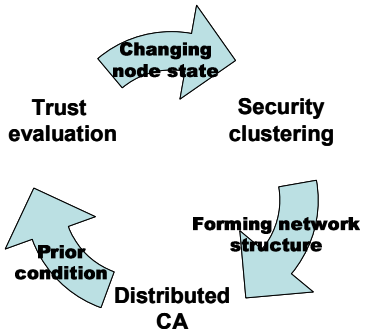

Figure 2. Relationship among trust evaluation, secure clustering and distributed CA

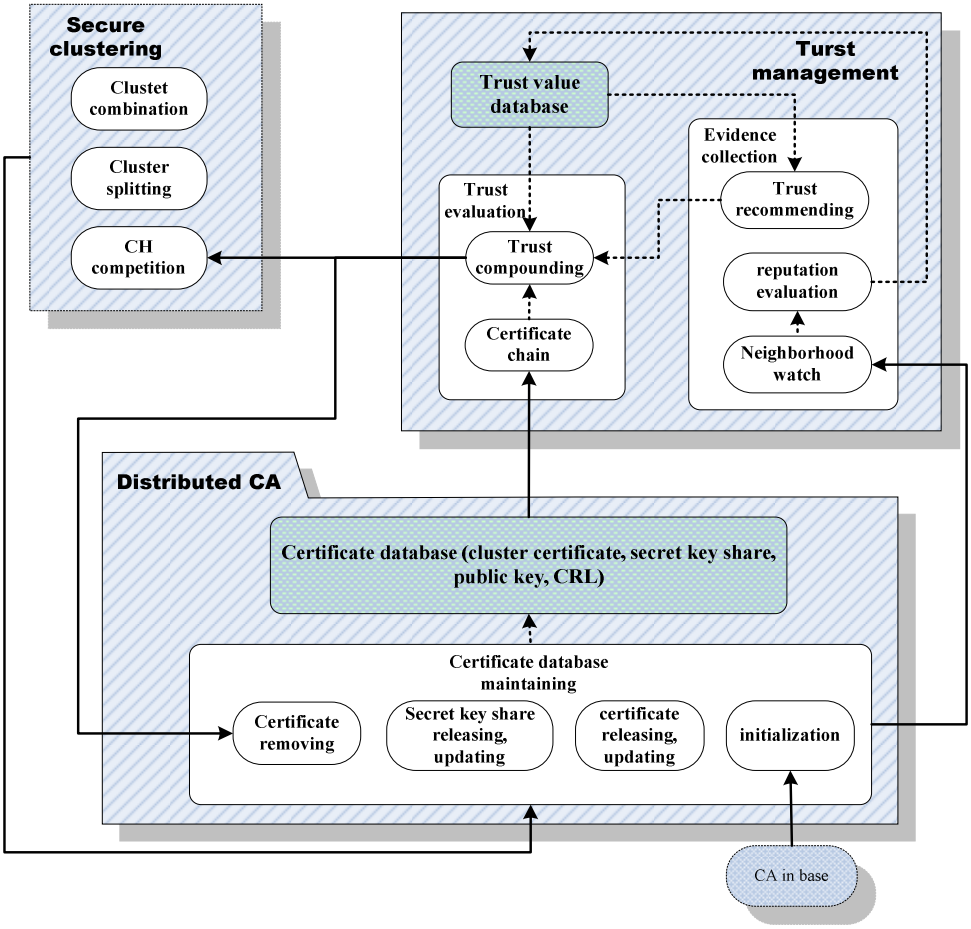

Figure 3. Distributed CA, Trust evaluation and secure clustering in the architecture

C. *Secure clustering.*

In [16], clustering protocols in the MANETs are grouped into six categories according to their objectives. *Dominating-Set-based (DS-based) clustering* tries to find a DS for a MANET so that the number of mobile nodes that participate in route search or routing table maintenance can be reduced. *Low-maintenance clustering* schemes aim at providing stable cluster architecture for upper-layer protocols with little cluster maintenance cost. *Mobility-aware clustering* takes the mobility behavior of mobile nodes into consideration. *Energy-efficient clustering* manages to use the battery energy

of mobile nodes more wisely in a MANET. *Load balancing clustering* attempts to limit the number of mobile nodes in each cluster to a specified range so that clusters are of similar size. *Combined-metrics based clustering* usually considers multiple metrics, such as node degree, cluster size, mobility speed, and battery energy, in cluster configuration, especially in cluster head (CH) decisions. With the consideration of more parameters, CHs can be more properly chosen without giving bias to mobile nodes with specific attributes. Also, the weighting factor for each parameter can be adaptively adjusted in response to different application scenarios.

In order to gain a more secure environment in MANETs, clustering should combine security scheme closely. Distributed CA should be deployed in cluster naturally. The trust value should be an important factor in the selection of CH (cluster head). The node whose trust value is lower than threshold should be excluded of network. Some clustering schemes [17-20] have been proposed partly considering the security goal. The relationship among trust evaluation, secure clustering and distributed CA is shown in Fig. 2.

The network is divided into clusters. Distributed CA is deployed in every cluster and responsible for the building of certificate chain between nodes inside the cluster. All CHs can form a distributed CA responsible for certificate chain between clusters. Thus, secure clustering forms the network model which is the basis of distributed CA. Distributed CA can build certificate chain for any two nodes either inside the same cluster or belong to different clusters. Certificate chain is prior condition for trust evaluation. Trust evaluation changes node's state in cluster which will influence the network model. The more detailed security architecture for tactical mobile ad hoc networks is shown in Fig. 3.

V. CONCLUSION

Security challenges and goals of tactical MANETs are analyzed and new security architecture is presented in this paper. The designing security architecture from a system viewpoint is the core. Main security technologies and their relationships are analyzed in detail.

REFERENCES

[1] S. Yu, Y. Zhang, C. Song, and K. Chen, "A security architecture for Mobile Ad Hoc Networks," http://blrc.edu.cn/blrcweb/publication/kc2.pdf, 2005.

[2] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in *Mobile Computing*, *Mobile Computing*, T. I. A. H. Korth, Ed.: Kluwer Academic Publishers, 1996, pp. 153-181.

[3] A. Dana, A. Yadegari, M. Hajhosseini, and T. Mirfakhraie, "A robust cross-layer design of clustering-based routing protocol for MANET," presented at Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, 2008.

[4] E. C. H. Ngai and M. R. Lyu, "An authentication service based on trust and clustering in wireless ad hoc networks: Description and security evaluation," presented at IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Jun 5-7 2006, Taichung, Taiwan, 2006.

[5] L. Eschenauer, V. D. Gligor, and J. Baras, "On trust establishment in mobile ad-hoc networks," presented at Proceedings of the Security Protocols Workshop, Cambridge, 2002.

[6] Sen, P. R. Chowdhury, and I. Sengupta, "A distributed trust establishment scheme for mobile ad hoc networks," presented at International Conference on Computing: Theory and Applications, ICCTA 2007, Mar 5-7 2007, Kolkata, India, 2007.

[7] J. Sen, P. R. Chowdhury, and I. Sengupta, "A distributed trust mechanism for mobile ad hoc networks," presented at ISAHUC' 06 - 2006 International Symposium on Ad Hoc and Ubiquitous Computing, Dec 20-23 2006, Surathkal, India, 2006.

[8] Y. Rebahi, V. E. Mujica-V, and D. Sisalem, "A reputation-based trust mechanism for ad hoc networks," presented at 10th IEEE Symposium on Computers and Communications, ISCC 2005, Jun 27-30 2005, Murcia, Spain, 2005.

[9] K. Wang, M. Wu, and S. Shen, "A trust evaluation method for node cooperation in mobile ad hoc networks," presented at International Conference on Information Technology: New Generations, ITNG 2008, Apr 7-9 2008, Las Vegas, NV, United States, 2008.

[10] Z. Lidong and Z. J. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, pp. 24-30, 1999.

[11] M. S. Zefreh, A. Fanian, S. M. Sajadieh, M. Berenjkoub, and P. Khadivi, "A distributed certificate authority and key establishment protocol for mobile ad hoc networks," presented at 2008 10th International Conference on Advanced Communication Technology, Feb 17-20 2008, Phoenix Park, South Korea, 2008.

[12] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," presented at IEEE ICNP 2001, Riverside,California,USA, 2001.

[13] S. Yi and R. Kravets, "MOCA:Mobile Certificate Authority for Wireless Ad Hoc Networks," presented at IEEE Proc of 2nd Annual PKI Research Workshop Program (PKI03), Gaithersburg,Maryland, 2003.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," presented at International Conference on Mobile Computing and Networking, Boston, Massachusetts, United States, 2000.

[15] C. Manikopoulos and L. Ling, "Architecture of the mobile ad-hoc network security (MANS) system," presented at Systems, Man and Cybernetics, 2003. IEEE International Conference on, 2003.

[16] V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust and recommendations in mobile ad hoc networks," presented at 3rd International Conference on Networking and Services, ICNS 2007, Jun 19-25 2007, Athens, Greece, 2007.

[17] A. Dana, A. Yadegari, A. Salahi, S. Faramehr, and H. Khosravi, "A New Scheme for on-Demand Group Mobility Clustering in Mobile Ad hoc Networks," presented at 2008 10th International Conference on Advanced Communication Technology, Phoenix Park, South Korea, 2008.

[18] J. H. Li, R. Levy, M. Yu, and B. Bhattacharjee, "A scalable key management and clustering scheme for ad hoc networks," presented at 1st International Conference on Scalable Information Systems, InfoScale '06, May 30-Jun 1 2006, Hong Kong, China, 2006.

[19] M. S. Bouassida, I. Chrisment, and O. Festor, "Efficient Clustering for Multicast Key Distribution in MANETs," presented at 4th International IFIP-TC6 Networking Conference: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems, NETWORKING 2005, Waterloo, Ont., Canada, 2005.

[20] E. C. Ngai and M. R. Lyu, "Trust- and clustering-based authentication services in mobile ad hoc networks," presented at Proceedings - 24th International Conference on Distributed Computing Systems Workshops, Mar 23-24 2004, Hachioji, Japan, 2004.

[21] Q. Zhang, G. Hu, and Z. Gong, "Maximum-objective-trust clustering solution and analysis in mobile ad hoc networks," presented at 3rd International Conference on High Performance Computing and Communications, HPCC 2007, Sep 26-28 2007, Houston, TX, United States, 2007.