Node-Level Information Security Monitoring for Mobile Ad Hoc Networks

Reijo Savola
VTT Technical Research Centre of Finland, Oulu, Finland
email: Reijo.Savola@vtt.fi

Abstract **–** Inherent freedom due to lack of central authority in self-organized mobile ad hoc networks introduces challenges to security and trust management. Arguably, trust management is the most critical security issue in mobile ad hoc networks. If nodes do not have any prior knowledge of each other, the trust establishment becomes complicated. In this kind of situations, the nodes themselves should be responsible of their own security. We propose a model for security management in self-organizing mobile ad hoc networks that is based on nodes' own responsibility of their security and node-level security monitoring.

Keywords *– security metrics, monitoring, mobile ad hoc networks*

I. INTRODUCTION

Dynamical communication is essential when attempting to monitor security critical situations dangerous conditions as early as possible. Mobile ad hoc networks (MANETs) [3] are networks that do not have an underlying fixed infrastructure and thus have to be self-organizing. In such networks, nodes co-operatively establish a network independently of any fixed common computational or storage elements or centralized management such as base stations. Different kinds of communication devices can act as nodes of MANETs, varying from tiny sensors to large computers. Mobile hosts can join the network on the fly and create a network of their own. Since an ad hoc network can be deployed rapidly with relatively low cost, it is a potential option for dynamical safety and security monitoring systems. Furthermore, self-organising networks survive better in war and terrorism scenarios compared to fixed critical infrastructures.

Among all the research issues, information security in MANETs is particularly challenging due to the highly dynamic network topology, the lack of central authority, the shared wireless medium, and memory and performance resource constraints. Despite the advances in the field, the research is lacking proposals to measure the overall security level of mobile ad hoc networks.

The main contributions of this work are in the analysis of basis for identification of suitable high-level information security metrics for mobile ad hoc networks and in the introduction of an on-the-fly security level estimation mechanism for MANETs to support both node-level and network-level decisions.

II. BACKGROUND

The nature of ad hoc networks makes them vulnerable to a number of attacks, such as denial-of-service, interference, impersonation, eavesdropping, information leakage and data tampering. In the following, we review the security goals and security environment of MANETs, discuss the scope of security, and provide an overview of security metrics.

A. Information Security in MANETs

The ultimate goal of the security solutions for mobile ad hoc networks is to provide services for the desired security needs, mainly *confidentiality*, *integrity*, *availability*, *authentication* and *non-repudiation*, at the desired security level. In general, the research has noted that traditional security solutions, such as public key infrastructures, or authentication mechanisms, are potential also for ad hoc networks, but in many cases they are not sufficient by themselves.

B. Security Metrics

Technical security metrics can be used to describe, and hence compare, technical objects. This includes algorithms, specifications, architectures and alternative designs, products, and as-implemented systems at different stages of the system lifecycle. Design vulnerabilities can result from an insecure design, whereas implementation vulnerabilities are connected to poor implementation of a product. Thus the former term typically refers to lower technology maturity. Security metrics model consists of three components: the *object* being measured, the *security objectives* (i.e. the "measuring rod" the object is being measured against), and the *method* of measurement. The security objectives typically consist of security requirements, such as specifications or standards, e.g. Common Criteria (CC) [2] Protection Profiles.

III. BASIS OF SECURITY METRICS FOR MANETS

A compositional approach can be used to define security metrics for MANETs, with the following, possibly iterative, steps [7]:

1. **Define security objectives:** the security objectives can be defined based on the knowledge of the security environment, assumptions and threats. Among other things, they should determine the required security level;
2. **Select component metrics** based on the security objectives;
3. **Find cross-relationships** (dependencies) between the component metrics and possibly re-define component metrics as independently as possible;

4. **Compose integrated security level information:** the final composition mainly depends on the method of measurement. The composition can be used for both *quantitative* and *qualitative* security metrics.

Critical control information distribution in a mobile ad hoc network means the location of the critical control information in that network with respect to time. The following main types of critical control information distribution can be identified:

- Trust information (e.g. keys, certicates, signatures),
- Routing information,
- Mobile entity identity information, and
- Packet forwarding information.

Security metrics can be developed from heuristics that compare the actual critical control information distribution to *a posteriori* knowledge of the most secure distribution of such information. The most secure distribution is the distribution the implements best the security goals. It is possible to develop predictive methods based on *a posteriori* knowledge.

In mobile ad hoc networks the cryptographic strength has tight cross-relationships with trust management, and often with other critical information management. There are various ways of describing cryptographic algorithm metrics, e.g. [4]:

- **Key length metric:** the security of a symmetric cryptosystem is a function of the length of the key. However, adding an extra bit does not always exactly double the effort required to break public key algorithms;
- **Attack steps metric:** attack steps is defined as the number of steps required to perform "the best known attack";
- **Attack time metric:** attack time is defined as the time required to perform the fastest known attack;
- **Rounds metric:** rounds are important to the strength of some ciphers;
- **Algorithm strength metric:** Jorstad and Landgrave [4] use algorithm strength as a name of a scale developed for expressing the overall measurement of a cryptographic algorithm's strength.

Generally, the most unexplored and the most critical field in security is the human user behaviour. Human factors have an enormous impact on the global security level of mobile ad hoc networks too.

An important consideration from the human user point of view is user acceptance, or, from a reverse perspective, *user resistance* to the systems with which they must interact. The user resistance manifests itself in various ways, including improper use of the security mechanisms [8].

When the technological solutions for routing. mobility and trust management become more mature, the effect of product quality will have more emphasis on the overall security level of mobile ad hoc networks. With mature technology we can investigate *implementation vulnerabilities*. Product quality metrics can be seen as a *general framework* for measuring mature solutions.

IV. ESTIMATION OF THE SECURITY LEVEL

In this section we propose an on-the-fly security level estimation mechanism for a networked monitoring system based on mobile ad hoc networks. The approach is self-organized with one exception: a hierarchy of trusted voting and countermeasure entities is required. If individual *trusted* nodes volunteer for these roles, the approach is self-organized. The objectives for the mechanism include the following:

- No central database can be used,
- Local monitoring in each node,
- Statistical knowledge of the security level is utilized,
- Measurement should be independent of the routing mechanism, and
- Decision mechanism to revocate the trust of suspicious nodes based on the observations of more than one node.

Clearly, there are two separate goals in the estimation process:

- Estimation of the security level of a *node*, and
- Estimation of the security level of the *network*.

A. Key Elements

In our estimation approach the key elements of the architecture are a Measurement Entity (ME) attached to each node, and a Voting Entity (VE). A Countermeasure Entity (CME) is also used for the Intrusion Detection functionality. The estimation is carried out in a mobile ad hoc network by co-operation between MEs and VEs.

A Voting Entity (VE) contains the same functionality as ME. In addition, it has an organizer role in case that that several MEs are going to make decisions concerning the security level and trustworthiness of a node. In an ad hoc network, certain trusted nodes can act as VEs.

A Countermeasure Entity (CME) acts on the results obtained from the voting process. Certain trusted nodes can act as CMEs.

Because critical information is distributed among MEs, VEs, and CMEs, a trust establishment and distribution mechanism is needed to enable the estimation and voting processes.

B. Estimation

The basic *node-level estimation* process is carried out continuously by the ME of the node. The ME uses the data stored in its metrics and reputation repository to estimate the current level of security from its own node point of view.

The critical information is updated in the reputation repositories of the MEs to support their *estimation of the security level in the network*. A VE can obtain update information from other VEs located in different parts of the network. General-level security updates to the MEs' metrics repositories can also be delivered using the VEs as a communication link.

At node level, MEs support the decision processes of the node, that use the security level information as an input. For example, the trustworthiness of a service may be assessed using the security level monitoring of ME.

C. Voting

There are a lot of situations where *democratic voting* can be used to support decisions to be made about the security level. For instance, if an ME detects a node with suspicious activity in the vicinity, voting can be used to justify countermeasures.

An ME can also inform a VE about its own security level estimates of an object. A voting process can be used to compare other MEs' observations of the same object.

A. Challenges

Mobile ad hoc networks are intrinsically resource-constrained, which makes our approach difficult to implement using the current technology. However, as the required level of security is often higher in cases where there are better memory and computation resources in use, the introduced approach is possible.

The selection of voting entities and countermeasure entities is also a problem in cases where complete self-organization of the network is a goal. Suitable trust establishment procedures are needed to select these trusted entities from a group of nodes. Trust management is also needed to enable the communication between the VEs, MEs and CMEs.

Suitable estimation algorithms should be developed for the metrics framework. This is a challenging task and requires a rigorous analysis of the metrics to be used.

As a long-time goal, general-level statistical knowledge has to be collected on: security algorithms, network products, user behaviour, applications, experiences from virus and worm attacks, etc. – about all critical issues contributing to the overall level of security.

V. RELATED WORK

The security level estimation mechanism presented here is closely related to the Intrusion Detection System (IDS) approaches proposed for mobile ad hoc networks. Mishra *et al*. [6] provide a state-of-the-art presentation of IDSs for mobile ad hoc networks. They conclude that application of IDSs to MANETs is a rather recent development, although in the wired world this research field has 15 years of tradition. The common problem in using IDSs for MANETs is the resource-constrained environment – our estimation mechanism suffers from the same complication. Zhang and Lee [9] describe a distributed and co-operative IDS model where every node in the network participates in the detection and response: the IDS agent runs at each mobile node. Bhargava *et al*. [1] propose an intrusion detection and response model to enhance security in the Ad Hoc On Demand Distance Vector (AODV) routing protocol. Kachirski and Guha [5] present an IDS based on mobile agent technology.

VI. CONCLUSIONS AND FUTURE WORK

We have discussed the problem of self-measuring the information security level in a mobile ad hoc network used as a dynamical communication basis for critical monitoring applications. Solving this problem clearly requires a multi-disciplinary effort. The current limited knowledge of the nature of security is hindering us from finding a rigorous solution. In this paper we have identified some major basis components that contribute to the security level of MANETs. The optimum management of critical control information distribution in time and placement in a mobile ad hoc network is seen as the major technical goal. Critical information includes, e.g., keys and certificates, routing information, identity information and packet forwarding control information.

Moreover, we have presented a security level estimation mechanism that can be used in a networked monitoring system, where a node has a lot of responsibility of itself and its neighbours.

Our future work will include further exploration of component metric areas and identification of the dependencies between them.

REFERENCES

[1] Bhargava, S. and Agrawal, D. P. Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks. In *Proceedings of IEEE Vehicular Technology Conference (VTC 2001) Fall*, Vol. 4, 2001, 2143-2147.

[2] *Common Criteria for Information Technology Security Evaluation*, v2.2, January 2004. Available at: www.csrc.nist.gov/cc/.

[3] *Internet Engineering Task Force (IETF) MANET Working Group*. At: www.ietf.org/html.charters/manet-charter.html.

[4] Jorstad, N. and Landgrave, T. S. Cryptographic Algorithm Metrics. In *Proceedings of the 20th National Information Systems Security Conference*, Baltimore, MD, 1997.

[5] Kachirski, O. and Guha, R. Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks. In *Proceedings of the IEEE Workshop on Knowledge Media Networks,* 2002, 153-158.

[6] Mishra, A., Nadkarni, K., and Patcha, A. Intrusion Detection in Wireless Ad Hoc Networks. In *IEEE Wireless Communications*, Feb. 2004, 48-60.

[7] Savola R. and Holappa J. Self-Measurement of the Information Security Level in a Monitoring System Based on Mobile Ad Hoc Networks. In: *Proceedings of the IEEE Int. Workshop on Measurement Systems for Homeland Security, Contraband Detection and Personal Safety*, Orlando, FL, USA, 29-30 March, 2005. 8 p.

[8] Schultz, E. E., Proctor, R. W., Lien, M.-C., and Salvendy, G. Usability and Security – An Appraisal of Usability Issues in Information Security Methods. In *Computer Security*, Vol. 20, No. 7, Oct. 2001, 620-634.

[9] Zhang, Y., and Lee, W. Intrusion Detection in Wireless Ad Hoc Networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom). Aug. 2000, 275-283.