Edith Cowan University

Research Online

Research outputs pre 2011

2005

Architecture for self-estimation of security level in ad hoc network nodes

Reijo Savola

Follow this and additional works at: https://ro.ecu.edu.au/ecuworks

Part of the Information Security Commons

Savola, R. (2005). Architecture for self-estimation of security level in ad hoc network nodes. In *Proceedings of 3rd Australian Information Security Management Conference* (pp. 88-94). Edith Cowan University. Available here.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ecuworks/7314

Architecture for Self-Estimation of Security Level in Ad Hoc Network Nodes

Reijo Savola
VTT Technical Research Centre of Finland
Reijo.Savola@vtt.fi

Abstract

Inherent freedom due to a lack of central authority of self-organised mobile ad hoc networks introduces challenges to security and trust management. In these kinds of scenarios, the nodes themselves are naturally responsible for their own security – or they could trust certain known nodes, called "micro-operators". We propose an architecture for security management in self-organising mobile ad hoc networks that is based on the nodes' own responsibility and node-level security monitoring. The aim is to predict, as well as to monitor the security level concentrating on the principal effects contributing to it.

Keywords

Security metrics, mobile ad hoc networks, security monitoring

INTRODUCTION

Mobile ad hoc networks MANETs (IETF) are networks that do not have an underlying fixed infrastructure and thus have to be self-organising. In such networks, the nodes co-operatively establish a network independently of any fixed common computational or storage elements, or centralised management such as base stations. 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 at relatively low cost, it has become an attractive option for both military and commercial uses. Among all the research issues, 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.

It is a widely accepted principle that an activity cannot be managed well if it cannot be measured (DeMarco 1982), (Kajava & Savola 2005). Without security measurements and metrics, the achieved security level hinges on guesswork. Many interdisciplinary factors affect this level, e.g. product quality, human factors, trust management, cryptographic strength, and chosen algorithms. We identify some security metric areas for MANETs, and present a security level self-estimation architecture for MANETs to support node-level and network-level decisions.

The rest of the paper is organised in the following way. Section 2 gives an overview of the security concerns of mobile ad hoc networks and an introduction to the related security metrics. Section 3 presents our security level self-estimation architecture for MANETs. After this, we present related work, followed by conclusions and discussion about future work.

SECURITY CONCERNS AND SECURITY METRICS OF 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. The nature of the basic mechanisms of the ad hoc paradigm makes ad hoc networks vulnerable. The following list points out the main properties of the ad hoc paradigm:

- Lack of central administration,
- Routing,
- Co-operation of algorithms,
- Variation in memory and computation resources, and
- Energy constrained operation.

In general, research has noted that traditional security solutions, such as public key infrastructures, or authentication mechanisms, are also a possibility for ad hoc networks, but in many cases they are not sufficient by themselves. Overviews of the research efforts can be found in (Hubaux et al. 2001), (Zhang & Lee 2000) and (Zhou & Haas 1999).

Security Concerns

There are major challenges in at least the three following important mechanisms:

- **Trust Management:** Authentication, Authorisation and Accounting (AAA);
- **Routing Management:** Secure routing,
- **Mobility and Identity Management:** Trusted information and identity management in mobility.

The following scenarios can be defined to classify MANETs from the security management point of view:

- **Operator controlled mobile ad hoc networks**: a trusted third partner (e.g. a network operator) provides central administration for the MANET. The central administration can be provided by a central node (*micro-operator)*, or through some coupling point with a fixed network (internet, intranet, cellular network, etc.).
- **Mobile ad hoc networks with no operator control**: the MANETs can form networks spontaneously without central administration. These MANETs can have a decoupling point with a fixed network, or they can form the decoupling at a later time. These MANETs are often temporary.

See Table 1 for a list of some threats to MANETs. Whilst all these threats can be malicious, some viruses and software bugs as well as inefficient routing and excessive data loading can be non-malicious too. Threats that are specific to both networks in general and MANETs concern the Application, Presentation, Session, Transportation and Network OSI (Open Systems Interconnection) Layers. In addition, active node impersonation, message replay, DoS (Denial of Service) and message copying/listening also potentially address the Data Link and Physical Layers. Viruses and Trojan horses attack the Application, Presentation and Session Layers. Software bugs can be present also on the Transportation and Network Layers. Last but not least, eavesdropping can occur on every OSI layer.

Table 1. *Some threats to MANETs and the countermeasures used*

Threat	**Used countermeasures**
Network threats:	
Active node impersonation	Node authentication
Message replay	Node authentication, message integrity
Denial of Service (DoS)	Node authentication, session authentication
Message copying / listening	Encryption
Inject erroneous messages	Node authentication, encryption
Distributed Denial of Service (DDoS)	Node authentication, session authentication
Message distortion	Message integrity
Message deletion	Non-repudiation
MANET-specific threats:	
Black hole	Node auth., encryption, secure routing protocols
Route information manipulation	Encryption
Old route information replay	Encryption
Inefficient routing	Network management, efficient routing
Excessive data load	Network management
Other threats:	
Virus	Anti-virus SW, SW updates, firewall
Trojan horse	Anti-virus SW, SW updates, firewall
Software bug	SW updates, firewall, SW testing tools
Eavesdropping	Encryption, transfer media planning

Security Metrics and Security Monitoring

Measurement can be defined as the determination of the magnitude of a quantity or as a systematic process of data collection, repeated over time or at a single point in time. Measurement practices in the field of security are not as well established as in some other fields (Sademies & Savola 2004).

The wide majority of available security metrics approaches have been developed for evaluating the maturity of security engineering processes. The most widely used of these maturity models is the Systems Security Engineering Capability Maturity Model SSE-CMM (ISO/IEC 21827). Another well-known model, Trusted Computer Security Evaluation Criteria (TCSEC, The Orange Book) (TCSEC 1985), expresses the security engineering process using classes and divisions as evaluation levels. Security metrics can be used to look for both design vulnerabilities and implementation vulnerabilities. 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 (Savola et al. 2005).

Examples of Measurable Security Components for MANETs

The most important component metrics areas in MANETs represent the security level of Trust Management, Routing Management and Mobility and Identity Management.

Arguably, trust management (trust establishment, distribution and revocation) in mobile ad hoc networks is currently the most critical and complex technical security challenge, having a strong impact on the overall security level. Zhou and Haas (1999) introduce the idea of distributing a Certificate Authority (CA) throughout the network, in a threshold fashion, at the time of network formation. In their threshold cryptography-based approach, the duties of CA (issuing, revoking, and storing of certificates) are distributed among the nodes. One more recent proposal includes self organised public key management (apkun et al. 2003). More state-of-the-art references can be found in Hubaux et al. (2001).

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. (Jorstad & Landgrave 1997):

- **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 (1997) use algorithm strength as the name of a scale developed to express the overall measurement of a cryptographic algorithm’s strength.

Generally, the most unexplored and most critical field in security is human user behaviour. 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. User resistance manifests itself in various ways, including improper use of the security mechanisms (Schultz et al. 2001). In general, systems with a poor usability design tend to evoke a greater degree of user resistance (Al-Ghatani & King 1999). Sophisticated usability metrics are non-existent for ad hoc network application scenarios. We refer the reader to general standards like (ISO/IEC 9126-4). Performance issues have a strong influence on the usability of mobile ad hoc networks. Other human factors include the level of security awareness, and resistance to social engineering. Social engineering means taking advantage of human fallibility. Due to the lack of comprehensive research results regarding human factors, we cannot develop sophisticated metrics for them. For the time being, metrics such as usability metrics and performance metrics form the baseline for metrics representing human factors.

In the case of mature technology we can investigate implementation vulnerabilities. Product quality metrics can be seen as a general framework for measuring mature solutions. In general, it can be concluded that the better the product quality, the better the level of security of that product However, it must be noted that there are a lot of situations where the requirements of the different quality attributes and security conflict – thus requiring a trade-off analysis as a solution. In the case of MANETs, the “product” is both a node in the network and the whole network.

The wireless environment uses an open medium for communications. This medium is freely available and is a serious threat, making the development of security solutions a challenging task. Wireless communications in general is a technical challenge, which has a strong effect on the global security level of MANETs.

Experience with virus and worm attacks has shown that the developers of malicious software programs tend to choose their target to be as widely used as possible. Based on this observation, it can be predicted that in the future more widely used mobile ad hoc network types will in general be more vulnerable to attacks than network types that are not so popular. The same applies to the size of the networks: the bigger the network, the more tempting it is for the attackers.

As a device at risk of being captured and hijacked, a mobile ad hoc network node must be protected in some way. The level of protection affects the level of security. The physical security of nodes can be severely compromised in some military applications of MANETs: nodes can be damaged or even destroyed completely.

SELF-ESTIMATION ARCHITECTURE

In this section we present an on-the-fly security level estimation mechanism for mobile ad hoc networks. The approach is self-organised 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-organised. 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,
- Measures should be independent of routing and
- There should be a decision mechanism to relocate the trust of suspicious nodes based on the observations of more than one node.

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.

Each ME in the network maintains an adaptive private metrics repository with the following information for each metric:

- **Metric objects:** a collection of measurable objects to be measured, e.g. a property in routing information messages;
- **Metric methods:** the methods associated with the metrics;
- **Metric measuring rod:** a database associated with the metrics that consists of reference information classified according to the level of security. The classification in the reference information may be based on quantitative or qualitative (using thresholds) reasoning.

The component metric areas discussed earlier can form the basic high-level structure for the private metrics repository. The measuring rod database can include security level data that is either generally known or gathered from statistical data. In this case, we assume that the data gathering and analysis was done beforehand – during the course of the actual node product development. In the future, data collection can be done by, e.g. security agencies or private companies.

In addition to the metrics repository, an ME maintains a private reputation repository of the network elements of a MANET or the elements that are visible to that particular node. The repository contains critical reputation information as input to the estimation process.

A Voting Entity (VE) contains the same functionality as an ME. In addition, it has an organiser role in the case 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.

Estimation Process

The ME of the node continuously carries out the basic node-level estimation process. 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. Moreover, the VE updates the MEs with information messages containing critical information about the changes in nodes and communication in the network vicinity. 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 the node level, MEs support the decision processes of the node that use the security level information as input. For example, the trustworthiness of a service may be assessed using the security level monitoring of an ME.

Voting Process

There are a lot of situations where democratic voting can be used to support decisions 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. As an example, let us consider a process for Intrusion Detection:

1. An ME detects suspicious activity in the neighbouring node;
2. The ME reports the findings to its VE;
3. The VE informs all its MEs; and they report their observations about the suspected node to the VE;
4. The MEs report their observations about the suspected node to the VE;
5. The results are gathered by the VE and delivered to the CME and back to the MEs;
6. The CME institutes countermeasures based on the voting results. For example, in the case of a remarkable threat, a node can be isolated from the network by invalidating its IP address; and
7. The MEs' trust level concerning the suspected node can be updated based on the voting results. The decision-making about this is left to each ME. In the case of a minor threat, however, the trust level can be reduced in the ME's reputation repositories.

An Implementation Example

A measurement system can be based on intra-node architecture of multiple sensors and analysers and a single manager entity to control them. The high level architecture inside a node (e.g. ME) consists of three main objects: Manager, Sensor and Analyser:

- **Manager** keeps track of all active sensors and analysers. It is responsible for starting and stopping the functionality of the Sensor and Analyser objects. Manager is only responsible for controlling the measuring objects and communicating with them and it does not contain any kind of counter-measure functionality. Manager can communicate with an external analysis application or module running on the node, which could handle the countermeasure and inter-node functionality if necessary.
- **Sensor** is an object controlled by a Manager object. Its purpose is to measure data from a measurement point and deliver it to the listening (one or more) Analyser object(s). For example, a Sensor object could measure battery voltage, address fields of used protocols, or the dropped packet count.
- **Analyser** gathers data from one or more sensor objects. Its purpose is to detect a specified security anomaly by analysing the data it receives from the Sensor(s). It has specified algorithms for analysing the data, and it can store data received from the sensors for later use in order to detect changes against history data. Analyser objects use the private metrics and reputation databases. An Analyser object usually has only one operational purpose – it can, e.g., detect a DoS attack by measuring the available bandwidth, packet loss ratio and payload readings from corresponding sensors.

An Analyser object can use other Analyser objects as sensors in some cases, for example an Intrusion Detection Analyser could use DoS and SDT (Sleep Deprivation Torture) Analysers to detect an ongoing intrusion to the system. The architecture in our proposal is scalable, allowing implementation on nodes with varying computing and energy resources.

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. These systems monitor audit data, look for intrusions to the system, and initiate a proper response. The communication architecture is similar to IDS, but there are some fundamental differences:

- The estimation is based on a collection of security metrics that mirror the overall security level of the network, whereas IDS typically concentrate on intrusions;
- The security level classification information is formed from statistical data;
- A node mainly carries out security level reasoning by itself;
- The security level information obtained from the estimation process can be used as input for the decision-making processes in a node, e.g. in making an application selection, or in choosing communication mechanisms; and
- As the nodes receive a lot of data on the security levels of different kinds of objects, democratic voting is valuable for making network-level decisions.

Mishra *et al*. (2004) provide a state-of-the-art presentation of IDS for mobile ad hoc networks. They conclude that the application of IDS to MANETs is a rather recent development, although in the wired world this research field has a 15-year history. The common problem in using IDS for MANETs is the resource-constrained environment – our estimation mechanism suffers from the same complication. Zhang and Lee (2000) 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.* (2001) propose an intrusion detection and response model to enhance security in the Ad Hoc on Demand Distance Vector (AODV) routing protocol. Kachirski and Guha (2002) present an IDS based on mobile agent technology.

CONCLUSIONS AND FUTURE WORK

Due to their nature MANETs are vulnerable to many additional threats as compared to legacy wireless networks. We propose an approach for security management in MANETs where node-level security monitoring plays an integral role in maintaining security.

We discussed the problem of measuring the overall security level of MANETs. Solving this problem clearly requires a multi-disciplinary effort. In this paper we have identified some major components that contribute to the security level of MANETs. Critical information includes, e.g., keys/certificates, routing information, identity information and packet forwarding control information.

Moreover, we introduced a security level estimation architecture where a node has a lot of responsibility of itself and its neighbours. The communication architecture is similar to Intrusion Detection Systems, but there are some fundamental differences in the metrics framework, security level classification and in applications. In addition to intrusion detection applications, the estimates generated by the mechanism can be used in node-level decision-making about applications and communication. Network-level security is increased due to the democratic voting mechanism of independent measurement entities, each independently aiming at a higher security level in the network.

Our future work will include further exploration of security issues in “pure” MANETs. Regarding security metrics, we will explore component metric areas and identify dependencies between them. Our initial framework will certainly be updated during the course of research.

REFERENCES:

Al-Ghatani, S. S., and King, M. (1999) Attitudes, Satisfaction and Usage: Factors Contributing to Each in the Acceptance of Information Technology. In Behaviour and Information Technology, 277-297.

Bhargava, S. and Agrawal, D. P. (2001) Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks. In Proceedings of IEEE Vehicular Technology Conference (VTC 01) Fall, Vol. 4, 2143-2147.

apkun, S., Buttyán, L. and Hubaux, J-P. (2003) Self-Organized Public-Key Management for Mobile Ad Hoc Networks. In IEEE Transactions on Mobile Computing, Vol. 2, No. 1, 52-64.

DeMarco, T. (1982) Controlling Software Projects. Yourden Press, New York.

Hubaux, J.-P., Buttyán, L., and apkun, S. (2001) The Quest for Security in Mobile Ad Hoc Networks. In: Proceedings of the 2nd ACM International Symposium of Mobile Ad Hoc Networking and Computing (MobiHoc), 146-155.

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

ISO/IEC 21827. (2002) Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM).

ISO/IEC 9126-4. (2000) Software Engineering – Product Quality – Part 4: Quality in Use Metrics.

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

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

Kajava, J. and Savola R. (2005) Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes. In: Proceedings of the European University Information Systems (EUNIS) 2005 – Leadership and Strategy in a Cyber-Infrastructure World Conference, 20-24 June, 2005, Manchester, UK. 6 p.

Mishra, A., Nadkarni, K., and Patcha, A. (2004) Intrusion Detection in Wireless Ad Hoc Networks. In IEEE Wireless Communications, Feb., 48-60.

Sademies, A. and Savola, R. (2004) Measuring the Information Security Level – A Survey of Practice in Finland. In: Proceedings of the 5th Annual International Systems Security Engineering Association (ISSEA) Conference, Arlington, Virginia, October 13-15, 2004, 10 p.

Savola, R., Sademies, A. and Holappa, J. (2005) A Brief Introduction to Measuring Information Security. In: Proceedings of the European Intensive Programme on Information Security Management and Technology (IPICS 2005), the 6th Winter School, Oulu, Finland, 30 March – 7 April, 2005. 6 p.

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

Trusted Computer System Evaluation Criteria TCSEC (1985) “Orange Book”, U. S. Department of Defense Standard, DoD 5200.28-std.

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

Zhou, L., and Haas, Z. J. (1999) Securing Ad Hoc Networks. In IEEE Network Magazine, Vol. 13, No. 6, Nov/Dec., 24-30.

COPYRIGHT

Reijo Savola ©2005. The author/s assign the School of Computer and Information Science (SCIS) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCIS & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.