Modeling Availability in Tactical Mobile Ad hoc Networks for Situational Awareness

Simon Hunke, Gabriel Klein, Marko Jahnke

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE
Neuenahrer Straße 20, 53343 Wachtberg, Germany
firstname.lastname@fkie.fraunhofer.de

Abstract: Mobile ad hoc networks (MANETs) provide a powerful technology to create self-organizing networks of mobile computing devices without existing infrastructures. In tactical deployment scenarios (e.g., disaster area rescue missions or military deployment), significant protection demands arise. To defend MANETs against internal and external attacks on the availability of its internal resources, it is necessary to achieve situational awareness (SA).

This contribution describes an extended modeling approach that represents the key properties of the observed environment in data structures. These enable the interpretation and prediction of the environment under different circumstances (e.g., under attack), using quantifiable security metrics. The enhancements described and discussed here cover shortcomings of earlier work, especially potential modeling inconsistencies in terms of objectively measurable availability values (e.g., on the physical layer).

1 Introduction

So-called tactical mobile ad hoc networks (tactical MANETs) comprise a number of mobile devices that communicate spontaneously via radio broadcast technology. Due to each node's ability to relay protocol packets for other nodes and the self-organizing determination of routes in the MANET (multi-hop routing), this technology provides great possibilities to utilize networking computer systems and distributed applications in areas where no fixed wired or radio communication infrastructure is available (yet).

Deployment scenarios for MANETs include tactical environments, such as military (e.g., command posts, infantry troops) and civil ones (e.g., disaster area rescue personnel, autonomous robot systems). Since information is broadcast using radio technology and since devices may also get lost during mission due to their small form-factors, both devices and the network need to be protected by means of resource-saving encryption as well as (potentially biometrics-based) user authentication. Due to the potential high level of criticality of the missions supported by the MANETs and due to the aforementioned enlarged attack surfaces, these networks have great protection demands, requiring not only preventive, but also monitoring (e.g., [JKW+08]) and response (e.g., [KRS+10]) capabilities.

Availability is a key requirement for tactical MANETs, because the nodes relay network protocol packets for each other and resources are very limited. Thus, resource availability

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

in MANETs is a property that needs to be maximized. In order to react to detected availability deficiencies (in cases of attacks and environment effects) some possibilities are the reconfiguration of the network topology, service and application instances, or the security policy, such as locking devices and forcing a user to reauthenticate. As the selection of a countermeasure and its respective parameters is important and challenging, the decision maker (e.g., the commander of the unit that operates the MANET) usually needs to be situation-aware. Necessary processes for situational awareness (SA[End00]) include the observation of the entities in the environment, achieving orientation and predicting the entity behavior for the near future. The model proposed in this paper supports all of these processes at least partially.

The rest of this contribution is organized as follows: Sect. 2 surveys some of the work that has been conducted in the field. In Sect. 3, an enhanced availability model is proposed and described in detail. Sect. 4 discusses its advantages and disadvantages and Sect. 5 concludes on the results so far.

2 Related Work

Implications of SA on Information Assurance (IA) with respect to implementation requirements have been discussed in several publications, e.g., [KBF+08]. Specific requirements for IA/SA in MANETs have been proposed in [LGBF05] as well as in [WJ08]. As a result, it can be stated that relevant information from multiple sources needs to be fused in order to achieve SA. This requires the utilization of different models (e.g., behavior models of the users and moving nodes) to support situation classification. Implementing SA in MANETs is not restricted to creating a global view on the network on one or more supervising nodes. Due to the (limited) autonomy of the distributed nodes, it seems also useful to create distributed operational pictures on the nodes of their respective environment according to their sensor observations.

More recent work [TS10] suggests to include mobility, energy state, connectivity, security and mission impact in a data model that is used as a basis for a visualization in order to make a decision maker situation-aware. Mutual trust between the MANET nodes is established using cryptographic authentication and the according trust values decrease until the next time a successful authentication process has been conducted.

Model-based impact assessment for intrusion response measures has already been investigated in [TK02]. Unfortunately, the proposed asset (or *resource*) model has not been flexible enough to include current and objectively measurable system-level information to support the SA process. Later, the methodology has been extended to be able to express more dynamics in terms of resource availability values ([Jah09], [JTM08]). The basic idea is as follows: For all DoS-relevant resources of interest in a system or network to be protected, the so-called *Common Operational Picture* (COP) is created and maintained as a representation of its functional model as well as the current state of the network. Based on the COP, it is not only possible to quantify the health of the network in terms of the availability of the user and mission resources, but also to determine the value and the costs of different alternative response actions by applying them on the data structures and

determine the resulting availability values. Different optimizations, e.g., in terms of response metrics optimization strategies [KOG+10], have been developed. It seems that the methodology is powerful enough to fulfill many of the requirements for IA/SA in tactical MANETs, especially if it is enhanced according to our suggestions in Sect. 3.

Other work extended the approach towards policy-based response enforcement [KDC+09] and to include security properties other than availability (i.e., integrity and confidentiality, [KDCB+09]).

3 Enhanced Availability Model for tactical MANETs

As reference scenario for achieving SA by utilizing our availability model we consider a MANET intended for a military infantry mission or a civil protection scenario. That means no central infrastructure is available and all devices come with capability for wireless communication in an ad-hoc manner, e.g., IEEE 802.11. Furthermore, we assume that the network is IP based and that a suitable ad hoc routing protocol (e.g., OLSR [CJ03]) is deployed. On every network node, a Voice-over-IP application (*VoIP*) for peer-to-peer voice communication and a command & control information system (*C2IS*) for displaying the geographical positions of all units involved are installed.

3.1 Modeling Technique

The graph-based modeling approach described in [Jah09] relies on a continuously updated COP of the systems to be protected. Here the COP consists of two parts: The *model graph* (or dependency graph) is constructed as a DAG $\hat{G} = (V, \hat{E})$ where the set of vertices V is associated with the resources. Edges $(r, s) \in \hat{E}$ exist where the availability of r depends on the availability of s. Each vertex is attributed with the function f_r that describes the dependency relationship of the vertex' resource to other resources. The vertices r in the *state graph* (or accessibility graph) $G = (V, E)$ are also associated with the resources, but they are attributed with their current normalized availability value $A(r) \in [0, 1]$ according to their definition. Edges $(r, s) \in E$ exist wherever s is currently accessibly by r.

Resources $r \in E$ may be specified on different levels of granularity, depending on the actual goal of the SA process to be implemented. On a high abstraction level, resources may include hosting locations or subnetworks. On a medium level, they could include host systems or network components as well as the links within the network and the applications and services on the network. Low-level resources might be subsystems of the operating system or functional modules of applications and services as well as hardware (sub-)components. For each of the resources, it is important to have a definition of its availability in terms of providing its intended service to the environment (e.g., request-response delays). Additionally, users $u \in V$ and the overall mission $m \in V$ that is to be supported by the network are also treated as resources.

The components of $\hat{G}$ and G are updated by performing on-line availability measurements and by interpreting availability-relevant event messages (e.g., from log files or monitoring

systems). The model graph reflects the way the network should currently work and the state graph depicts its actual current state which might differ from the model. Propagation algorithms aid the completion of missing availability values wherever measurement data is missing or incorrect. Due to the simplicity of the data structures, the computation effort is relatively low, as long as the model itself is consistent.

3.2 Overview of Enhanced MANET Model

In [JTM07] an availability model based on the modeling technique described above has been developed for a small tactical MANET scenario, but the model has not been validated so far. In addition, it relies on end-to-end measurements for the determination of certain availability values which do not scale well for MANETs. For that reason we have extended the existing model to better meet the requirements of this specific kind of network by adding further resources, in particular for low-level connectivity aspects.

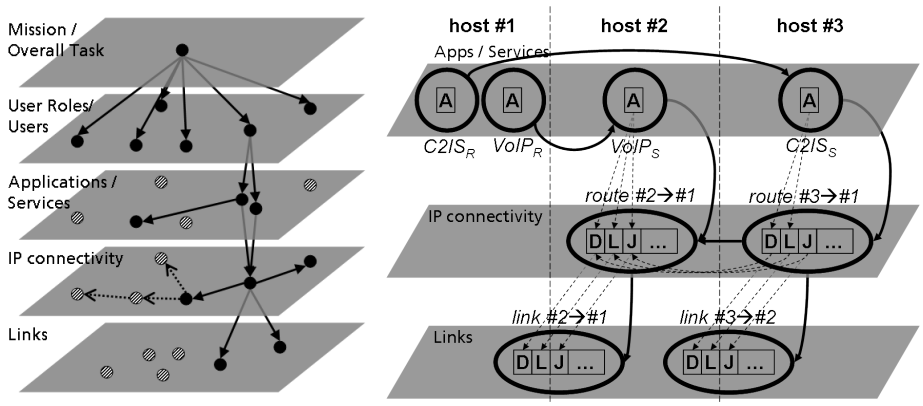

Figure 1: Overview of the enhanced MANET availability model. Left: Layered model graph $\hat{G}$. Right: Availability vectors in state graph G for determining end-to-end connection properties with distributed measurements.

The left side of Fig. 1 illustrates an overview of our new model derived by systematically applying the graph-based modeling approach to the underlying MANET scenario. The top level resource is the mission as it constitutes the higher context. The users rely on the software applications installed on the mobile devices for accomplishing their tasks in the context of the common mission. Both the VoIP application and the C2IS are two distinct resources on the applications/services layer. Since they are peer-to-peer applications, they depend on other peers (arrows on the same layer) and on the IP stacks for communicating with these peers (arrows down to IP connectivity layer). In addition, the ability of a resource at the IP connectivity layer to reach a certain destination depends on the link to the next hop on a route to the destination and on the ability of the next hop to reach the destination. Therefore the dependencies at the IP connectivity layer reflect the routing topology of the MANET and allow for relying on only local measurements in order to determine the availability of all resources.

It should be noted that the system resources of the mobile devices, such as OS, CPU, memory, etc., are not included in the model explicitly as we assume that in a tactical scenario the network is the bottleneck and more restrictive to the availability than the system resources. However, if there is an evidence that the system resources are exhausted the availability of the affected resources representing the apllications can be adjusted accordingly.

3.3 Modeling Shortcomings and Enhancements

One shortcoming of the approach so far is that it entirely relies on normalized availability values $A(r) \in [0, 1]$. An example where these values cannot be used appropriately is the area of low-level connection characteristics, as will be shown in the following.

Regarding the communication, applications have non-functional requirements, e.g., QoS requirements, and need specific properties of the communication channel, such as a certain packet delay, packet loss, and jitter. For example, real-time voice over IP requires low delay, jitter, and packet loss whereas a C2IS for geographical position information sharing works well with moderate delay and packet loss; in this case jitter does not matter at all. The availability value of a resource, representing the IP connectivity (middle layer on the right side of Fig. 1), has to reflect how well these requirements are fulfilled in order to determine the availability value of the dependent resources, i.e., the applications. As we want to avoid end-to-end measurements, which are not appropriate for MANETs, the technical characteristics of a path in the network, like delay, loss and jitter, would have to be modelled as virtual resources at the link layer. However, the utilization of normalized availability values is not possible in general as shown below. For reasons of simplicity, we will only consider delay in our further discussion of this aspect.

For one-hop paths the delay, transformed into an availability value by normalization to $[0, 1]$, is identical to that of the corresponding radio link. With regard to paths with more than one hop, some availability values have to be aggregated. For that purpose, it is a mandatory precondition that the normalization of the delay is strictly monotonic because otherwise, the result of the aggregation becomes ambiguous. However, this is not always true as the example of a VoIP session over a one-hop path illustrates. Up to a certain threshold – about 150ms – a user will probably not notice the delay at all and perceives the application as fully available. That means, a constant availability value of 1 follows from all delay values less than the given threshold. But even if the normalization of the link delay were approximated by a strictly monotonic function (e.g., by a sigmoid function), an error is induced for every link on a path what could render an application unavailable ($A(r) = 0$) which is in fact available.

Therefore the propagation of normalized values is not appropriate when modeling low-level physical properties in combination with thresholding. Distributed applications may have certain threshold requirements for end-to-end connections in terms of delay, loss, and jitter. Thus, for determining whether these thresholds are exceeded in an end-to-end manner, the raw parameters need to be aggregated and the result needs to be checked against the thresholds. This is not possible when using normalized abstract quality parameters for the connections. □

ISBN 978-3-88579-286-4

To address the shortcomings mentioned above, the enhanced model proposed here allows for using arbitrary values for availability in vector shape, e.g., $A(r) \in \mathbb{R}^n$, refered to in the following as *availability vector*. This extension to the modeling approach enables the calculation of statistics for a path in the network between a source-destination pair by providing the necessary information by means of the availability vectors of the appropriate resources. For modeling a link one resource is sufficient, since it can carry all information, e.g., delay, loss, etc., in its availability vector (see right side of Fig. 1). However, for each source-destination pair, there needs to be a distinct resource at the IP connectivity layer, as every path may have its own characteristics. According to the requirements of the applications, the availability vectors for the paths can be transformed into the availability values for the applications in the original sense, i.e., $A(r) = f_r(A(s_1), \ldots, A(s_p)) \in [0, 1]$ for $A(s_1) \in \mathbb{R}^{n_1}, \ldots, A(s_p) \in \mathbb{R}^{n_p}$.

Additionally, a structural refinement is necessary, since both applications utilized in the aforementioned tactical scenario are peer-to-peer applications, and therefore the corresponding resources of one type mutually depend on each other as any can act as a server and a client as well. Without any further refinements, this would yield cyclic dependencies that would inhibit the availability propagation algorithm. This can be avoided by splitting the resources for a peer-to-peer application into a sending part and a receiving one and letting the latter depend on the former, as suggested but not further discussed in [Jah09].

4 Discussion

The model proposed in the previous section can be regarded as basis for achieving situational awareness with respect to availability. It allows the assessment of the network characteristics, of the availability perceived by the user during their operation of the applications, and of the corresponding impact on the mission success. In principle, it enables a decision maker (human or machine) to identify availability deficiencies. The corresponding information could be used for the selection of reaction or optimization measures such as reconfigurations of the network or application instances. But that aspect is out of the scope of this paper.

According to the SA information requirements, the model is not comprehensive though because it just illustrates the effects of DoS attacks and does not comprise the reasons. This is due to the fact that an attack is a discrete event which may have an impact on the model graph or the values contained in the availability vectors, but it has no functionality any other resource relies on, so that an attack is not appropriate to be modeled as resource. In order to achieve in-depth SA, it is necessary to integrate the proposed availability model and all related information – e.g., IDS alerts – in an overall approach for reasoning about the reasons of an availability degradation. In this context, it is a particular aspect to allow for the discrimination between an overload situation and an attack.

ISBN 978-3-88579-286-4

5 Conclusion

This contribution has proposed an enhancement of a graph-based availability model for tactical MANETs that relies completely on local measurements for the availability determination. Therefore, low-level connectivity properties had to be modeled. For that purpose, it is useful to extend the original modeling technique by introducing availability vectors for propagating objectively measurable availability-related parameters, such as link-layer delays. Our future work will comprise the validation of our model, w.r.t. its costs and adaptability to dynamics of the network, and its integration into an overall approach to IA/SA for MANETs.

Our current efforts at the creation of a global operational picture for reproaching it with a supervising node (e.g., a commander). Further work might also address local operational pictures which are maintained by each node individually.

References

[CJ03] T. Clausen and P. Jacquet. RFC 3626: Optimized Link State Routing Protocol (OLSR). http://www.rfc.org, 2003.

[End00] M. Endsley. Theoretical Underpinnings of Situation Awareness: A Critical Review. In *Situation Awareness Analysis and Measurement*, pages 317–341. Mahwah, 2000.

[Jah09] M. Jahnke. *Graph-based Automated Denial-of-Service Attack Response*. PhD thesis, University of Bonn, 2009.

[JKW+08] M. Jahnke, G. Klein, A. Wenzel, N. Aschenbruck, E. Gerhards-Padilla, P. Ebinger, S. Karsch, and J. Haag. MITE – Manet Intrusion Detection for Tactical Environments. In *Proc. of the NATO/RTO IST-076 Research Symposium on Information Assurance for Emerging and Future Military Systems*, Ljubljana, Slovenia, 2008.

[JTM07] M. Jahnke, C. Thul, and P. Martini. Graph based Metrics for Intrusion Response Measures in Computer Networks. In *Proc. of the 3rd LCN Workshop on Network Security. Held in conjunction with the 32nd IEEE Conference on Local Computer Networks (LCN2007)*, Dublin, Ireland, October 2007.

[JTM08] M. Jahnke, C. Thul, and P. Martini. Comparison and Improvement of Metrics for Selecting Intrusion Response Measures against DoS Attacks. In *Proc. of the GI Sicherheit2008 Conference*, Saarbrücken, Germany, April 2008.

[KBF+08] R. Kemmerer, R. Büschkes, A. Fessi, H. König, P. Herrmann, S. Wolthusen, M. Jahnke, H. Debar, R. Holz, T. Zseby, and D. Haage. Dagstuhl Manifesto: 08102 Outcome Working Group – Situational Awareness. In *Proc. of the Perspectives Workshop on Network Attack Detection and Defense*, Leibniz-Zentrum für Informatik, Wadern, Germany, 2008.

[KDC+09] N. Kheir, H. Debar, F. Cuppens, N. Cuppens-Boulahia, and J. Viinikka. A Service Dependency Modeling Framework for Policy-Based Response Enforcement. In *Proc. of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA2009)*, Como, Italy, 2009.

[KDCB+09] N. Kheir, H. Debar, N. Cuppens-Boulahia, J. Viinikka, and F. Cuppens. Cost evaluation for intrusion response using dependency graphs. In *IFIP/IEEE international conference on Network and Service Security*, 2009.

[KOG+10] G. Klein, A. Ojamaa, P. Grigorenko, M. Jahnke, and E. Tyugu. Enhancing Response Selection in Impact Estimation Approaches. In *Proc. of the MCC2010 Military Communications and Information Systems Conference*, Wroclaw, Poland, September 2010.

[KRS+10] G. Klein, H. Rogge, F. Schneider, M. Jahnke, J. Tölle, and S. Karsch. Response Initiation for Distributed Intrusion Response Systems in Tactical MANETs. In *Proc. of the European Conference on Computer Network Defense (EC2ND)*, Berlin, Germany, October 2010.

[LGBF05] J. Lefebvre, M. Gregoire, L. Beaudoin, and M. Froh. Computer Network Defence Situational Awareness Information Requirements. Technical report, Defence R&D Centre, Ottawa, Canada, December 2005.

[TK02] T. Toth and C. Kruegel. Evaluating the impact of automated intrusion response mechanisms. In *Proc. of the 18th Computer Security Applications Conference (ACSAC'02)*, 2002.

[TS10] J. Treurniet and M. Salmanian. Challenges in Visualizing Situational Awareness in a Tactical Military Mobile Ad Hoc Network. In *Proc. of the NATO/RTO Workshop on Visualising Networks: Coping with Chance and Uncertainty*, Rome, NY, USA, October 2010.

[WJ08] S. Wolthusen and M. Jahnke. Information Assurance Situation Awareness for Tactical MANETs. In *Proc. of the NATO/RTO IST-076 Research Symposium on Information Assurance for Emerging and Future Military Systems*, Ljubljana, Slovenia, 2008.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html