Efficient Trust Authority Distribution in Tactical MANET Environments

Steffen Reidt
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Email: s.reidt@rhul.ac.uk

Stephen D. Wolthusen
Norwegian Information Security Laboratory
Gjøvik University College
N-2818 Gjøvik, Norway
and
Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Email: stephen.wolthusen@rhul.ac.uk

***Abstract*— Determining the efficiency of protocols in MANET environments depends heavily on accurate characterization of the operating environment, particularly of message complexity. In this paper we therefore describe an extensible group mobility model intended to capture platoon-level light infantry operations, characterized by a hierarchical set of evolutions. Movement in this model is further constrained by a terrain model reported in previous work, allowing for a more precise modeling and simulation of algorithms on tactical networks. We subsequently describe a mechanism for disseminating key revocation information across a distributed trust authority (TA) in which nodes may be compromised or exhibit Byzantine failure. We propose and evaluate key revocation mechanisms to optimize the requirements of fast revocation propagation, complete coverage, and low message complexity in the previously described modeling and simulation environment.**

I. Introduction

Key revocation is a basic and essential element of security architectures such as a public key infrastructure (PKI) or identity based public key cryptography (ID-PKC). In one of the first publications on security in ad hoc networks, Zhou and Haas presented an overview of a security architecture which already discusses the need for public key revocation of a node is no longer trusted [1], although without providing actual details. Later work elaborating the use of (k, n)-threshold cryptography and thus especially a subset of nodes as certificate authority either neglects key revocation entirely [2] or most commonly use flooding algorithms for this purpose [3]. Considering the frequent usage of flooding for key revocation, Go *et al.* evaluated the performance of flooding in MANETs [4], reaching the conclusion that better and more promising schemes for distributing information in ad hoc networks must be designed. In this paper we therefore focus on disseminating revocation information across trust authority (TA) nodes in a mobile ad hoc network. In earlier work we have developed a scheme for the efficient distribution of a trust authority in tactical networks [5]. This cluster based distribution scheme facilitates the determination of the TA nodes under the configuration of adaptable functions, which may e.g. consider battery powers, topological location in the network, and trust relations between nodes. Since the mobility of the nodes significantly influences the frequency of changes in the TA and the connectivity in the network, a realistic model of the nodes' mobility is decisive for the analysis of revocation distribution schemes. Although network simulators have been an essential element of research in mobile ad hoc networks for about ten years, mobility models are still surprisingly limited with the most commonly used model being a random waypoint model in which nodes traverse randomly appointed positions in a defined free space area. Since all statements about a real behavior of MANETs which are based on an unrealistic scenario are questionable, we initially develop a suitable mobility model for tactical networks incorporating both environmental constraints and tactical doctrine. The remainder of this paper is structured as follows: In section II we give an overview of existing mobility models and then describe our newly developed group mobility model, which is designed particularly for modeling group movements in tactical networks in section III. Section IV defines a new distribution scheme for key revocation based on a TA as provided by the scheme in [5]. The scheme is then

1-4244-1513-06/07/$25.00 ©2007 IEEE

evaluated in a scenario modeled by the new mobility model is then simulated in section V. In section VI, the efficiency of key revocation under the new scheme is compared with a naïve flooding algorithm as used by other schemes. Finally, section VII discusses our ongoing and planned extensions to the model and algorithms for efficient and robust TA distribution in tactical MANET environments.

II. Related Work

Mobility Models: Research in mobility models has resulted in a number of models ranging range from probabilistic to completely deterministic ones. Random mobility models represent (almost) probabilistic models since the movements of the nodes is only bound to a few parameters such as the variance of a Gaussian distribution or some constraints which keep the nodes in a bounded area; see [6] for a survey and simulation-based comparison of several random mobility models and [7] for a concise categorization of mobility models in general. One of the most utilized probabilistic models is the *Random Waypoint Model* [8], [9], where nodes trace positions which are determined by a uniform distribution. Since the nodes in this model use the shortest path to reach their aim, node density in the center of the simulation area is higher than in marginal regions. The *Random Direction Model* [10] attempts to avoid this behavior by sending the nodes on a detour via the border of the simulation area. Further models such as the *Gauss Markov Mobility Model* cause a random movement by spontaneous changes of the direction of nodes. All of these random models are configurable by few parameters such as the variance of the Gaussian distribution and provide popular basic mobility models for network simulators. A more deterministic movement strategy is provided by the *Graph Model* [11], which restricts the nodes to move randomly on predefined trails. Extensions of this model are commonly used in mobile vehicular ad hoc networks (VANETs), where the nodes (cars) are stopping at a cross-ways to simulate traffic lights [12] or move smoothly through curves [7].

Initial work on topography aware mobility models was done by Jardosh [13]. In Jardosh's *Obstacle Mobility Model* buildings are modeled as polygons and the transmission between two nodes is interrupted or highly attenuated if their line of sight is intersected by a polygon. The nodes are either allowed to walk on predefined trails, or reach their randomly defined aim by the shortest pathway through the obstacle-area. All previously described mobility models treat the nodes independently and thus do not provide any group movement, as required especially in tactical networks. A generalization of these models are group models [14], [15], where every node moves relative to the logical center of the group, while this logical center can be provided by any of the models above.

Several basic implementations, especially of the random mobility models, can be found in network simulators. In this paper we use the simulator *NS-2* [16], which offers the possibility to either create totally deterministic movements by writing every single movement directly in the simulation script, or to generate a random waypoint scenario with the script *setdest*. More modular and reusable software for this purpose is provided by the tools *BonnMotion* [17] and *CanuMobiSim* [18]. Both tools are Java-based mobility generators, which provide several random models as well as the possibility to generate mobility files for the common network simulators *NS-2*, *GlomoSim* [19] and *QualNet*. Moreover, CanuMobiSim provides a Graph Model, where the graph can either be read from a separate file or directly from an XML file. Due to this added functionality exploited in our extended mobility model in section III, CanuMobiSim was chosed as the basis for our implementantion. Several strategies for group formations, especially in military operations, are described in [20]. The hierarchical structure of fire teams up to platoons has been integrated into our implementations and some of the formations established the basis for the analysis of our key revocation scheme on a TA in section VI.

III. A Mobility Model for Tactical MANETs

In tactical mobile ad hoc networks expected to be used in military and emergency response networks, the participants (nodes) are likely to move in groups, which split up, coalesce, and lose or add single members. As noted in section II, a number of random mobility models for pairwise independent node movements have been developed, while the investigation of group mobility models is basically limitted to the Reference Point Group Mobility Model (RPGM) [14] and e.g. a somewhat rudimentary implementation n the NS-2 simulation files. In this section, we extend the idea of the RPGM and report on a new *Coalition Mobility Model* (CMM), which is designed to be used in conjunction with our topography aware propagation model [21] (both for use on the mobile nodes and to provide more realistic simulation). The doctrine for the tactical movements of military formations as described in [20] are hierarchically organized. Formations are arrangements of soldiers and organized

subgroups in relation to each other. Leaders choose formations based e.g. on their analysis of the terrain, the likelihood of enemy contact, and the need for speed. The smallest group in an infantry operation is the *fire team*. Fire teams are likely to consist of four soldiers, that follow the orders of the team leader. *Squads* as the next group in the hierarchy and consist of fire teams and the squad leader. Squad formations describe the relationships between fire teams in the squad. Finally *platoons* present the highest group in this hierarchy and consist of squads in special formations, the platoon leader and other additional soldiers such as the platoon sergeant or a machine gun crew.

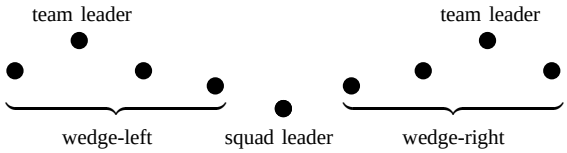

Fig. 1. Squad line

Figure 1 shows one possible formation for an squad, that is organized as a line to provide maximum firepower. In order to enable the creation and flexible formation change of arbitrary tactical units, our implementation of the CMM contains a flexible and reusable definition of a group. The entire mobility model, including the groups with their different formations, are defined in a XML file. A group, as considered in the CMM is defined in EBNF as follows:

distance	=	”real number”
angle	=	”real number”
name	=	”string”
node	=	distance angle
formation	=	name {{node} {group distance angle}}
group	=	name formation {formation}

According to this definition, every node has a fixed desired position in its formation, which is described by the distance to the group center and the angle relative to the direction of group motion. A formation itself can not only contain nodes, but also complete subgroups that are also relatively positioned to the group center via distance and angle. Finally a group contains at least one formation. In the case of fire teams, squads and platoons for example, the the *group* “fire team” could contain several formations with four *nodes*. The higher level *group* “squad” could then consist of two fire teams and an additional *node* as “squad leader”, while the highest level *group* “platoon” could consist of *nodes*, fire team *groups* and squad*groups*.

Finally, for completion of the CMM the movement of the group centres needs to be defined. We use an extension of the Graph Model, which has allready been implemented in the mobility framework CanuMobiSim by Stepanov *et al.* The nodes in this model are restricted to walk on edges of a connected graph, i.e. there exists a path between every two vertices in the graph. In Stepanov’s graph model [22], every node chooses the next destination vertex uniformly distributed under all vertices and traces its aiming point on the shortest path. Given that pathways in tactical networks are typically not chosen randomly, and for the purpose of simulating well-specified scenarios, the routes in CMM are predefined. Moreover, the CMM supports the consideration of several groups with independent configurations, such that e.g. several taskforces could walk on predefined routes, while small groups of independently tasked soldiers walk randomly on the graph. The CMM deliberately does not consider the influence of the topography as buildings or vegetation. Feasible realizations, such as nodes bouncing on housewalls or finding the shortest path quoin by quoin, are not realistic, while more suitable models tend to be very complex and are subject of ongoing research. Instead we propose the consideration of the topography separately during the simulation calculation. According to a predefined topographical area, the edges of the graph and reasonable group-configurations can be determined manually.

Implementation: We have implemented the CMM as an extension of the framework CanuMobiSim [18], which already contains random mobility models and a graph mobility model. An essential feature of CanuMobiSim is the configuration of the respective mobility model in a XML file. We have extended the scope of this XML file to include the description of groups and additional parameters for the CMM. The configuration strategy of a group as defined in EBNF above allows the re-use of groups in arbitrarily depth and thus enables an almost deterministic, but still manageable setup of the CMM. Further extensions of the CMM, such as the changing of nodes between groups or the collection of nodes, will be implemented as required.

IV. Key Revocation in Tactical MANETs

Since every node in a MANET needs to be able to ascertain whether a public key has been revoked, a key revocation certificate must be spread to all nodes that might potentially hold it. An easy possibility that obviates any additional communication is the incorporation

of an expiration date in the public key [23]. Unfortunately, this approach is not sufficient for MANETs since nodes need to be able to revoke keys before they expire, e.g. in the case of key compromise or malicious behavior. In the case of a public key revocation of an ordinary node it might be sufficient to inform a m-hop neighborhood of the revocation as proposed by Hoeper [24]. We will investigate the minimum communication overhead for revoking the key of ordinary nodes in future work. Within the scope of this paper we examine the revocation of a public key from a TA node, which must be disseminated across all TA nodes in the network. As noted before, there are two reasons for explicit key revocation of an TA node. In the first case a TA node notices that its own key has been compromised and revokes the key itself. The second possibility is that an ordinary node observes a suspicious behavior of its TA node[1], or its TA node has changed to an ordinary node. In both cases the node will change its TA connection and inform the new TA node about the suspicious behavior of the former one. If a TA node receives at least δ independent messages about suspicious behavior of another TA node, it will revoke the key of this node. Thus a public key from a TA node can only be revoked by a TA node and accordingly our scheme for TA key revocation starts at a TA node. This behavior is mandatory, since the ability of ordinary nodes to revoke public keys of TA nodes would facilitate a revocation attack [25].

Revocation distribution scheme: Our distribution scheme for revocation information is based on the scheme on the distribution of a trust authority in tactical networks [5]. This cluster-based TA-distribution scheme establishes an overlay network, in which every node is either a cluster head (TA node) or connected via d hops to a TA node. We have extended this scheme by adding information about connections to TA nodes to already exchanged packets, so that every TA node knows its TA neighbors. A TA neighbor in a d-hop cluster algorithm is a TA node, that is not more than $2d + 1$ hops away, e.g. at most $2d$ nodes form the connection between the neighboring TA nodes. Note that in a connected network every TA node has almost one TA neighbor. As a simplified example, figure 2 illustrates the TA overlay for the squad from figure 1.

Based on this information we define our distribution scheme for revocation information as follows:

[1]Every node either connects to a TA node (its TA node / TA connection) or is a TA node itself. See [5] for the underlying TA distribution scheme.

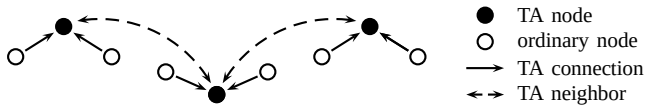

Fig. 2. 1-hop overlay network for the squad line

1) A TA node sends the revocation information packet (RIP) and revocation nodes list (RNL) to all its TA neighbors. The RNL contains the IDs of its neighboring nodes, e.g. the nodes that shall receive the RIP in this first step.
2) If a TA node receives a RIP it forwards the packet to all its TA neighbors that are not contained in the RNL and the P-RNL. The private RNL (P-RNL) is an additional table in which every node locally stores the Ids of the nodes, which it already forwarded the RIP. Before forwarding the RIP, the IDs of the neighbors and the P-RNL are added to the corresponding RIP.

The algorithm terminates once every node holds only a RIP with a corresponding RNL that contains all the IDs of its TA neighbors. The communication between the TA nodes is based on the underlying routing protocol since the usage of gateway nodes is for efficiency resons not intended by the trust authority distribution scheme [5]; the performance of this distribution algorithm is compared with the corresponding flooding algorithm in section VI. This flooding algorithm, which we additionally implemented in NS-2, uses the same strategy as the algorithm above, with the only difference being that the TA neighbors are replaced by real physical neighbors.

V. Simulation

With the help of the key revocation algorithm and a realistic simulation scenario it is now possible to investigate the propagation speed of the revocation information in the network. For the simulation we use a mobility model created by the CMM from section III in combination with the topography aware propagation model that we developed in [21]. During the following simulation it was configured to consider the interruption of transmission by buildings as well as reflection effects up to a depth of 2. Figure 3 shows four screenshots of the simulation scenario, which was visualized with our extension of the NS-2 visualization tool iNSpect [26].

The simulation starts with a platoon in column formation that consists of 32 nodes moving towards a complex of buildings. As nodes in these simulations are typically represented by infantry on foot, average speed of the group was set as 2 m/s, while nodes are able to increase

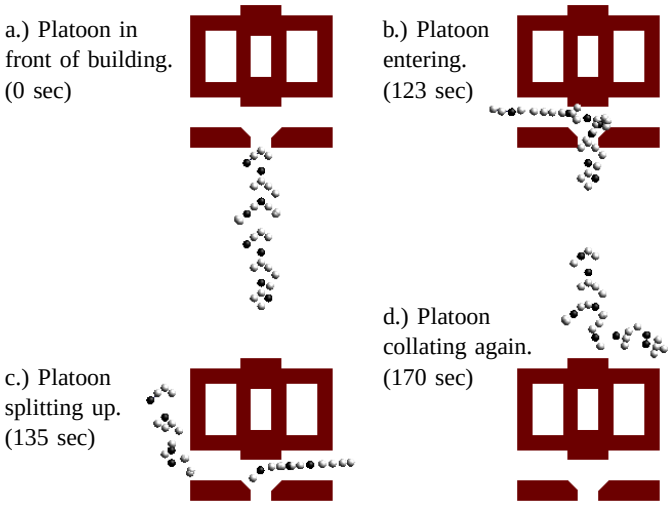

Fig. 3. Simulation scenario combining topographical propagation model and CMM

their speed up to 3 m/s to build up or keep desired formation. Ordinary nodes are represented by grey dots, while the members of the TA are black. The average distance of neighboring nodes in this scenario is 10m, and the width of the building is 140m. In figure 3, the platoon has reached the building in the fixed formation column in which the TA overlay network dwells on a constant set of nodes. While the platoon is moving between the buildings, it changes its formation, splits up to circle the building and finally re-forms a column in the back of the building again. This variation in formations as well as the influence on the radio wave propagation by the buildings causes connection breakdowns or new connections between nodes and thus also effect the choice of the TA nodes.

VI. Analysis

In section IV we introduced an algorithm for key revocation on the one hand based on TA neighbors and on the other hand based on real physical neighbors yielding a flooding algorithm. In this section we will now compare these two algorithms in terms of communication complexity and distribution time, and furthermore highlight other interesting results of the simulation scenarios.

Initially, the nodes in the platoon need to determine the subset of nodes that will represent the TA. The period of this process is dependent on the mobility of the nodes in the network and the frequency of cluster messages. Different choices of the cluster message frequency of 2,4 and 8 seconds yielded almost the same results in this very constantly arranged network. For further analysis, we used the results of the simulation with a cluster message frequency of 4s. In this simulation setup, the TA reaches a constant state after less than 30s, i.e. 5 rounds of cluster message exchanges. The nodes in front of the building (simulation time of 0s) have already reached this state in which 8 nodes are chosen as TA nodes. During the entire simulation, the number of TA nodes ranges between 7 and 9, while most of the time dwelling at 8 TA members. The transmission power of the nodes, which directly influences the number of TA nodes, was chosen to be 0.2mW yielding a transmission range of approximatelly 20m. The transmission range decreases due to the consideration of the ground in the radio propagation model with a increasing distance d as $1/d^4$. An amplificiation of the transmission power to 1mW, respectively causes a increase of the communication range by 50% from 20 to 30 metres. As a result of this increased connectivity in the network, the number of TA nodes diminishes to 5 or 6. A similar impact on the choice of the TA nodes is exerted by the influence of the topography in the simulations. Due to reflection effects between the two buildings, the propagation power is amplified by up to 100%. This effect can be identified in figures 3.2 and 3.3 where the distance between two TA nodes in the stretched formation is significantly higher than in figures 3.3 and 3.4.

For the purpose of measuring the times for the two key revocation distribution algorithm, we have implemented the flooding algorithm in NS-2. The decisive factor for the propagation time of the revocation information is the forwarding time period of the nodes, which includes acknowledge, processing and sack of the packet and is by default set to 0.1s in NS-2. The results of the algorithm based on TA neighbors were calculated on the assumption that the underlying routing protocol has already established the required routes between the TA nodes. Table I shows the number of sent as well as received packets and the distribution time for all 8 revocations during the simulation. The distribution time was measured as the time period between the initial sending and the earliest time at which all TA nodes have received the information. The left value in each column shows the results for the flooding algorithm (A1) and the right value for the TA neighbor based algorithm (A2), respectively.

Both algorithms in the example I are nearly equivalent in terms of the distribution time. This behavior can be explained by the fact that the propagation time is mainly influenced by the forwarding time period of the nodes and thus by the maximum number of hops which are required to reach the TA nodes. Under the assumption

Time [sec]	sent p.		received p.		distribution time	
	A1	A2	A1	A2	A1	A2
20	10	7	54	36	0.630	0.642
44	11	7	58	41	0.748	0.642
116	3	3	18	18	0.224	0.218
124	4	3	21	16	0.226	0.218
132	3	4	12	13	0.216	0.324
160	3	3	15	17	0.222	0.318
196	3	2	15	10	0.222	0.212
232	11	6	55	34	0.638	0.536

TABLE I

COMPARISON OF DISTRIBUTION ALGORITHMS FOR REVOCATION INFORMATION

that both algorithms find an almost optimal path to the most distant TA nodes, this number of maximum hops will differ only slightly. In the case of a separated group which only consists of approximately 15 nodes, the number of sent and accordingly received packets in both schemes is almost equal as well. However, in case of a complete group size of 32 that can be seen at the measurements 1,2 and 8, the communication expense is significantly reduced. Note that the algorithm based on TA neighbors does not necessarily reach all nodes, but only the TA nodes, while the flooding algorithm unnecessarily forwards the information to all nodes. Hence, the choice of the TA neighbor based algorithm is recommendable for networks with more than 30 nodes and a topology in which the TA nodes have central positions in the network.

The assumption of centrally positioned TA nodes is essential for the efficiency of the algorithm. In networks not satisfying this assumption it is possible to create clusters in which a flooding algorithm will reach all nodes faster and with less communication overhead than our revocation algorithm. An interesting question for 1-hop clusters is, if every flooding algorithm which operates only on the centrally positioned cluster heads needs less broadcasts than the corresponding flooding algorithm on all nodes. Note, that a flooding algorithm executed only on the cluster heads of a 1-hop cluster is allready a flooding algorithm for the whole network.

However, within the scope of this paper we are not focusing on the efficiency of flooding algorithm in general, but on a reliable and within our cluster algorithm efficient algorithm for disseminating revocation information to the TA nodes. The behavior of the cluster algorithm was examined in the simulation scenario 3 in the former section, as well as in further simulations [27] for 1-hop clusters, and showed the desired and configured behavior to choose centrally positioned clusterheads. According to these simulations, the revocation algorithm reaches all TA nodes with less communication overhead than usual flooding algorithm which are intended to reach all nodes. All these simulations were based on 1-hop clusters, but in case of d-hop cluster algorithm with $d \geq 2$ the revocation algorithm can benefit even more from the short number of nodes that need to be contacted. Since the communication in the revocation algorithm is based on the underlying routing algorithm, it furthermore benefits from more reliable communication. As an extension of this algorithm we investigate the incorporation of responses on received packets to ensure a complete distribution of the revocation information in future work.

VII. CONCLUSION

In this paper we have describe and analyzed schemes for disseminating key revocation information across a distributed trust authority in a tactical MANET environment. As a realistic analysis of the revocation scheme requires a precise characterization of message complexity and the location of the distributed trust authority nodes to ensure that security-related constraints are satisfied, we first introduced the coalition mobility model (CMM) for simulating platoon-level movements. Based on an overlay network of TA nodes, which is determined by a scheme for TA distribution from former work [5], we proposed a key revocation mechanism to optimize the requirements of fast revocation propagation, complete coverage, and low message complexity. We built up a simulation scenario in NS-2 in which a platoon changes formations and splits up and re-forms again owing to topographical influences. The comparison of our TA-based scheme with a flooding algorithm showed that the additional information provided by the overlay network can provide significant performance benefits, particularly if the total number of nodes is larger in relation to the number of TA nodes. The application of a realistic mobility scenario, including structured formation changes, demonstrated many advantages for the behavior of the network and the corresponding TA overlay network. As an example, the frequency of cluster messages could be reduced to 8 seconds, while it is usually chosen to 0.2 seconds in cluster algorithms suitable for random mobility models. The high density of the nodes and relatively constant formations in tactical networks allow reductions of transmission power and dynamic adjustment of the number of TA nodes. In order to avoid any unintentional

changes of the number of TA nodes, we will investigate the configuration of the transmission power and other parameters during the simulation in future work where particular attention will be given to using knowledge of planned future events and movements to influence TA algorithm distribution and behavior.

Source code for the implementation of the CMM as well as videos of node mobility and TA behavior is available from the authors by request.

ACKNOWLEDGMENT

Research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

REFERENCES

[1] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, November-December 1999.

[2] M.Bechler, H.J. Hof, D. Kraft, F. Pahlke and L. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 4, Hongkong, 2004, pp. 2393–2403.

[3] S. Yi and R. Kravets, "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks," in *Proceedings of the 2nd Annual PKI Research Workshop*, 2003.

[4] H. W. Go, P. Y. Chan, Y. Dong, A. F. Sui, S. M. Yiu, Lucas C. K. Hui and Victor O. K. Li, "Performance Evaluation on CRL distribution using Flooding in Mobile Ad Hoc Networks (MANETs)," in *ACM-SE 43: Proceedings of the 43rd annual Southeast regional conference*. New York, NY, USA: ACM Press, 2005, pp. 75–80.

[5] Steffen Reidt and Stephen D. Wolthusen, "Efficient Distribution of Trust Authority Functions in Tactical Networks," 2007.

[6] T. Camp, J. Boleng and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," *Wireless Communications & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, no. 5, pp. 483–502, 2002.

[7] Christian Bettstetter, "Smooth is Better than Sharp: A Random Mobility Model for Simulation of Wireless Networks," in *Proceedings of the 4th ACM International Workshop on Modeling, Analysis and Smulation of Wireless and Mobile Systems*, Rome, Italy, 2001, pp. 19–27.

[8] William Navidi and Tracy Camp, "Stationary Distributions for the Random Waypoint Mobility Model," *IEEE Transactions on Mobile Computing*, vol. 3, no. 1, pp. 99–108, 2004.

[9] Christian Bettstetter, Giovanni Resta, and Paolo Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, pp. 257 – 269, 2003.

[10] E.M. Royer, P.M. Melliar-Smith, L.E. Moser, "An Analysis of the Optimum Node Density for Ad hoc Mobile Networks," in *ICC 2001. IEEE International Conference on Communications*, vol. 3, 2001, pp. 857–861.

[11] J. Tian, J. Haehner, C. Becker, I. Stepanov and K. Rothermel, "Graph-based Mobility Model for Mobile Ad Hoc Network Simulation," in *Proceedings of 35th Annual Simulation Symposium*, San Diego, California, 2002, pp. 337–344.

[12] Niranjan Potnis and Atulya Mahajan, "Mobility Models for Vehicular Ad Hoc Network Simulations," in *Proceedings of the 44th Annual Southeast Regional Conference*, Melbourne, Florida, 2006, pp. 746–747.

[13] Amit P. Jardosh, Elizabeth M. Belding-Royer, Kevin C. Almeroth and Subhash Suri, "Real-world Environment Models For Mobile Network Evaluation," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, pp. 622– 632, March 2005.

[14] Xiaoyan Hong, Mario Gerla, Guangyu Pei and Ching-Chuan Chiang, "Mobility Models for Vehicular Ad Hoc Network Simulations," in *Proceedings of the 2nd ACM International Workshop on Modeling, Ynalysis and Simulation of Wireless and Mobile Systems*, Seattle, Washington, United States, 1999, pp. 53–60.

[15] Ken Blakely and Bruce Lowekamp, "A Structured Group Mobility Model for the Simulation of Mobile Ad Hoc Networks," in *Proceedings of the second international workshop on Mobility management & wireless access protocols*, Philadelphia, PA, USA, 2004, pp. 111–118.

[16] "NS-2." [Online]. Available: http://www.isi.edu/nsnam/ns/

[17] "BonnMotion." [Online]. Available: http://web.informatik.uni-bonn.de/IV/Mitarbeiter/dewaal/BonnMotion/

[18] "CanuMobiSim." [Online]. Available: http://canu.informatik.uni-stuttgart.de/mobisim/

[19] "GlomoSim." [Online]. Available: http://pcl.cs.ucla.edu/projects/glomosim/

[20] Headquarters, United States Department of the Army, "Field Manual FM 7-8: Infantry Rifle Platoon and Squad," U.S. Government Printing Office, Apr. 1992.

[21] Steffen Reidt and Peter Ebinger and Stephen D. Wolthusen, "Resource-Constrained Signal Propagation Modeling for Tactical Networks," 2006.

[22] Illya Stepanov, Pedro Jos Marrn and Kurt Rothermel, "Mobility Modeling of Outdoor Scenarios for MANETs," in *Proceedings of 38th Annual Simulation Symposium*, San Diego, CA, 2005, pp. 312–322.

[23] Dan Boneh and Matthew K. Franklin, "Identity-Based Encryption from the Weil Pairing," in *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*. London, UK: Springer-Verlag, 2001, pp. 213–229.

[24] Katrin Hoeper and Guang Gong, "Key Revocation for Identity-Based Schemes in Mobile Ad Hoc Networks," in *ADHOC-NOW*, 2006, pp. 224–237.

[25] Haowen Chan, Virgil D. Gligor, Adrian Perrig and Gautam Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 02, no. 3, pp. 233–247, 2005.

[26] "iNSpect." [Online]. Available: http://www.igd.fhg.de/igd-a8/de/projects/mobsec/inspect

[27] Steffen Reidt and Stephen D. Wolthusen, "An Evaluation of Cluster Head TA Distribution Mechanisms in Tactical MANET Environments," 2007.