An Evaluation of Cluster Head TA Distribution Mechanisms 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*— Trust authority (TA) services are both important infrastructure services for layered protocols requiring the availability of an identification and authentication mechanism such as access control mechanisms and confidentiality services, and can also be viewed as exemplars for the secure and efficient distribution of computations in general. While such general problems have been studied extensively, tactical MANET environments impose a number of requirements and constraints such as RF range and cost, battery limitations, and computational capabilities which call for more specific approaches. In this paper we report the analysis of algorithms for TA service distribution based on cluster head algorithms and improvements on the basic algorithms based on the specific requirements as identified in the course of simulations of tactical scenarios and realizing appreciable increases in efficiency over the general case in the process.**

I. Introduction

Security architectures often tacitly assume the availability of cryptographic services, which may not be the case for mobile ad hoc networks (MANETs). Trust authority (TA) services form the basis for many advanced services, and the bootstrapping and their continued availability represent a significant challenge from both efficiency and security perspectives, particularly in hostile environments such as tactical networks. Such networks are self-organizing, self-discovering, rapidly changing in topology and devoid of dedicated infrastructural elements, and must cope with both active adversaries and limited resources such as energy, bandwidth, and computational power for services for both public key infrastructures (PKI) or for identity-based (ID-PKC) systems. Recent research has investigated the issue of establishing a PKI on a subset of nodes in the network [1], [2] based on the use of cluster algorithms for the determination of cluster heads. Simultaneously, numerous authors have focused on the propagation of trust and developed models for establishing trust in MANETs [3], [4], [5], [6], [7]. In this paper, we report on the efficiency gained by combining such cluster algorithms with selected additional metrics, including trust, battery capacity of participating nodes, and metrics pertaining to the underlying network, namely cost of routing, bandwidth requirements, and desirable per-hop signal strengths. This provides robust criteria for the distribution of data (e.g. key material) and computation across nodes in a dynamic MANET as required for a distributed trust authority.

The remainder of the paper is structured as follows: Section II provides a brief overview of cluster algorithms and existing work on security architectures. Section III then introduces the extension of our distribution model, which describes the augmented configuration possibilities for the underlying cluster algorithm. Two simulation scenarios are then described in section III, while section V provides a comprehensive analysis and evaluation of the distribution algorithm based on these simulations. Finally, section VI discusses our ongoing and planned extensions to the model and algorithms for efficient and robust TA distribution in tactical MANET environments.

II. Related Work

Overlays and Clusters as a Structuring Mechanism for Information Collection and Dissemination

In the recent years clusters have been widely utilised to determine subsets of mobile ad hoc networks under

the objective of saving energy [8], enhancing routing protocols [9], [10], finding efficient flooding [11], [12], and broadcasting mechanism [13], or to generally build low-cost backbones [14]. Clusters have also been applied in recent research on distributing trust authorities in ad hoc networks [1], [2].

Bechler [1] establishes a security architecture using clustering and (k, n)-threshold cryptography, but does not consider trustworthiness. In each cluster, exactly one distinguished node, the cluster head, is responsible for establishing and organizing the cluster. Clusters are formed as geographically needed: If nodes cannot find existing clusters, they create some themselves, with existing clusters being merged and split on demand. A further drawback in Bechlers work is the significant relevance of gateway nodes, which act as connectors between neighbored clusters. As Bechlers simulation results illustrate, 34.2% of the overhead traffic is produced by the gateway nodes, whereas the cluster heads only produce 47.5% of the overhead traffic, although they incur the management of the security shares. The frequency of changes of the clusterheads is not considered at all in Bechlers work, instead leaving clusterhead are supposed to delegate their role to another node in the cluster. A breakdown of one cluster head causes a complete rebuild of the cluster and thus a downtime and considerable communication overhead.

Lin-Jiun [2] also builds a cluster-based security architecture for MANETs and avoids the issue of trust establishment assuming that every node has already exchanged a public key and a session secret key with its direct neighbors. Since we assume wireless data transfer, there is no reason why these initially exchanged keys should be trustworthy, calling the underlying assumptions into question. Lin-Juin utilizes Amis' cluster algorithm for the determination of the cluster heads, that appeared in our simulations to change the cluster heads quite frequently. However, Lin-Juin's security architecture does not examine the changing of cluster heads or the frequency of those changes at all.

Previously we have addressed the issue of establishing a trust authority under the consideration of configurable metrics for trust, energy level and arbitrary further functions [15]. For this purpose we modified Amis' [16] cluster algorithm, replacing the node id as the decisive factor in his algorithm by a *quality factor*. This quality factor provides the key for the configuration of our distribution algorithm and demonstrated its impact in an example for sufficient energy handling[15]. Amis' cluster algorithm comes, due to the avoidance of gateway nodes, with the advantage of independently changing clusterheads, i.e. one change does not activate a chain of further changes. Nevertheless, several simulations figured out that the mobility of the network provokes quite frequent changes of the cluster heads, which is an infeasible behavior in the scope of a trust authority. Resent research has investigated the incorporation of additional mechanism to control the changes of cluster heads.

III. A CLUSTER BASED ALGORITHM FOR TRUST AUTHORITY DISTRIBUTION.

Previously [15] we described an algorithm for trust authority distribution in tactical networks. We developed a variant of Amis' [16] cluster algorithm for determining the cluster heads, which represent the members of the trust authority. The special feature of our algorithm is the *quality factor* that describes the belief of a node i about a node $j's$ qualification for being a TA node. This value is used by our modification of the cluster algorithm to decide about the choice of the TA nodes[1]. We have also defined several metrics for the configuration of the quality factor and illustrated how the consideration of the battery level helps to keep the nodes on similar battery levels and thus prevent the early breakdown of nodes.

First simulations have shown the tendency of the cluster algorithm to change the cluster heads quite frequently. One possibility for the prevention of this behavior provides the quality factor, which can be configured to assign a higher quality to TA nodes and thus facilitate their reelection. However, this would be a misuse of the quality factor that would decrease its potency for more sensitive configuration issues such as energy level and trust values. We have therefore augmented the cluster algorithm itself by mechanism for avoiding abrupt changes of the cluster heads. These mechanism will be introduced in the remainder of this section. Our original cluster algorithm was defined in [15] as follows:

- Each node collects the information broadcast by neighbors and retains this until it is refreshed or exceeds its predefined lifetime. Cluster information with a `hopsToGo` value greater than 1 are pushed on the stack `forwardInfo`, whereupon the respective `hopsToGo` value is decreased by 1.
- In certain (possibly node-specific) time periods each node determines all quality factors about his known d-hop neighbors, choosing the node with the highest quality factor as its cluster head. *If the node itself holds this value, or if another node has chosen him*

[1]For consistency, cluster heads are labeled as TA nodes.

as cluster head, the node will itself be a TA node. The node then broadcasts the newly determined TA status, its additional information such as the battery level and `forwardInfo` to its neighbors. Every entry of the `forwardInfo` stack contains a parameter `hopsToGo`, i.e. the number of forwarding hops, initially set to cluster depth.

The highlighted part of this definition briefly describes the decision procedure, which provides the anchor for a more sophisticated decision strategy. Firstly we augmented the possible set of trust authority states `TA_MEMBER` and `NO_TA_MEMBER` by `TA_ASPIRANT` and `LEAVING_TA`. The `TA_ASPIRANT` parameter is utilized to insert a second step in the process of getting a TA member. According to this, a node firstly changes its state to `TA_ASPIRANT` if he holds the highest quality value under its neighboring nodes. After a certain configurable period `CONSTANT_TA_INTEREST` as TA aspirant the node will then get a TA member if it still holds the highest quality value. The respective mechanism is utilized with the help of the parameter `CONSTANT_NO_TA_INTEREST` for the state `LEAVING_TA` to avoid a abrupt release of the `TA_MEMBER` state.

A further and most effective change on the algorithm is the incorporation of a delay mechanism in the process of changing the TA connection. According to this, a node only connects to a new TA node, and thus obliges this node to be a TA member, if the interest in this connection exists for a certain time period `CONSTANT_CONNECTION_INTEREST` or if its old TA connection suddenly dropped out. Furthermore, a node is only interested in a new connection if the quality of the potentially new TA node exceeds the quality of its current connection by a threshold amount `MINIMUM_QUALITY_DIF`. During the simulations which are introduced in the following section, the parameters `CONSTANT_TA_INTEREST` and `CONSTANT_CONNECTION_INTEREST` were set to 3 times the cluster message frequency. The parameter `CONSTANT_NO_TA_INTEREST` which is responsible for decelerating the process of leaving the TA status, appeared to drastically bar the nodes from leaving the TA and was finally set to 0. The value of the parameter `MINIMUM_QUALITY_DIF` was set to 0.1.

The choice of TA connections as utilized by the cluster algorithm does not necessarily establish real TA connection in the later security architecture. In the scope of the cluster algorithm a node can immediately connect to another node, which may require an interval to establish its state as a TA member. The TA connections in scope of the real network need to be chosen under the additional consideration of the effective ability to provide the TA service. According to this, our cluster based algorithm for trust authority distribution provides a sufficient subset of TA nodes, which can then be used for bootstrapping the security architecture on top of these nodes, but also as independent as necessary from any structures from inside the distribution algorithm.

IV. Simulation

The optimization of the algorithm for trust authority distribution, as elaborated in the former section, is based on several simulation scenarios. Two of these scenarios, modeling possible group movements in military task forces, are introduced in this section. The simulations were performed with our extension of the network simulator NS-2[17], including the topography aware radio propagation model[18] as well as the cluster algorithm for trust authority distribution. The ray optical propagation model, which is originally developed for the utilization on single devices, can therefore also be used as a propagation model from the scope of the network simulator. During the following simulations it was configured to consider the interruption of transmission by buildings as well as reflection effects up to a depth of 2.

We used iNSpect[19] for visualization purposes in which the consideration of new tracefile entries, such as required for the trust authority information, is comfortably realizable. The first simulation (figure 1) contains 35 nodes approaching an urban area, splitting up in groups of at least three nodes and re-grouping. The second scenario (figure 2) a group of 37 nodes traces a route through hostile area and performs formation changes accordingly. In both simulations the group is organized as a platoon in which the common distance of neighboring nodes is 10m. Movement techniques for traveling, enemy contact and crossing danger areas of platoons were motivated by [20]. As nodes in these simulations are typically represented by infantry on foot, averages speed of the group was set as 2 m/s, while nodes are able to increase their speed up to 3.5 m/s to build up or keep desired formations. We chose transmission power of the nodes to 5 mW, yielding due to the underlying Two ray ground model a maximum communication range in free space of approximately 45m. Ordinary nodes are represented by grey spots, while the members of the trust authority are presented by black spots.

Simulation 1 is intended to expose the influence of abrupt communication breakdowns as well as of the di-

Fig. 1. Simulation 1: Platoon of soldiers tracing a city area.

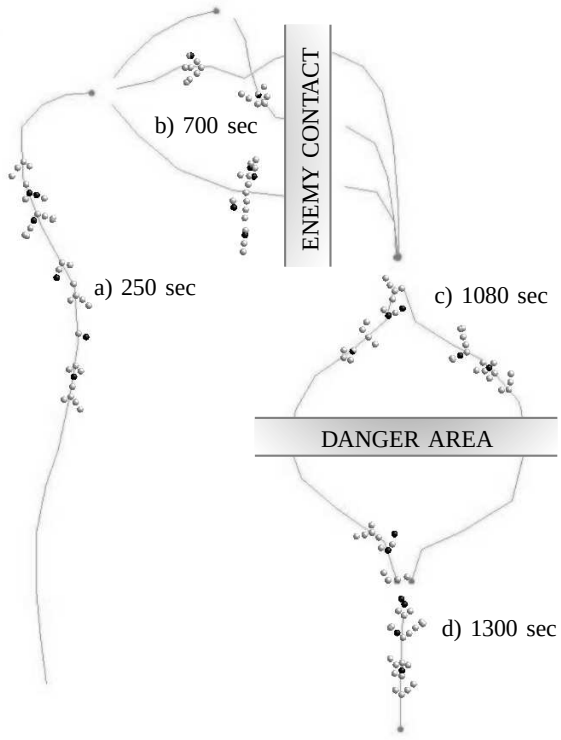

Fig. 2. Simulation 2: Platoon of soldiers traveling through hostile area.

vision of the network in several smaller groups. The simulation area as illustrated in figure 1 measures $600x900$m and the simulation time is $850s$. Figure 1a) shows the imminent devision of the platoon in three squads after reaching the city area. The nodes have decreased the distances between each other from typically 10 metres to 5 metres yielding a more compact network. $110s$ later (figure 1b)) the squads trace independent routes in between the buildings, while several fireteams temporary leave the squad to occupy further streets. Finally the squad falls back into formation on leaving the urban area.

Simulation 2 is intendend to expose the influence of redeploying the platoon while traveling, node failure and insulate contacts after enemy contact and network devision into two groups while crossing a danger area. The simulation area as illustrated in figure 1 measures 700 x 900 metres and the simulation time is 1350 seconds. Our extension of iNSpect also allows the construction of pathways, which are illustrated by grey lines in the background. The platoon of 37 nodes starts traveling with a speed of 2 m/s and stretches while accelerating up to 3 m/s (figure 2a)). Due to expected enemy contact, the platoon splits up short time later, two squads following the lower path, while the remaining two squads trace the upper two paths. At second 700 the lower two squads change their formation due to enemy contact to a line (figure 2b)). During this procedure which takes 120 seconds, the nodes are moving with an average speed of 0.1 m/s and their wireless devices are likely to incur insulate contacts or drop out totally. Thereupon, after collating to a platoon again, the group divides to cross a danger area (figure 2c)) and forms up a traveling platoon again (figure 2d)).

V. Analysis

In section III we have discussed the changes in our cluster based algorithm for trust authority distribution, while the former section introduced two simulation scenarios that were used to figure out these optimizations. In this section we will now illustrate the resulting behavior of our cluster based distribution algorithm regarding to three aspects:

1) Total number of TA nodes (cluster heads)
2) Number of nodes successfully connected to TA
3) Number of received packets/s

The first aspect describes the number of TA nodes at every time in the simulation scenarios and shows the influence of formation changes, interaction of radio waves with the topography and the transmission power

on the total amount of TA nodes. Since our trust authority distribution algorithm is intended to perform the basis for a security architecture in which several secret shares are distributed among the TA members, the number of TA nodes is a decisive factor.

The number of nodes that are successfully connected to the trust authority helps to draw conclusions about the sufficient information exchange in the network. We define a node to be successfully connected to the trust authority if its TA node is indeed a member of the TA and the physical connection is still existent. The continuous exchange of cluster packet would yield a perfectly informed network and thus enable every node to immediately react to connection breakdowns and changes in the behavior of neighboring nodes. However, since transmission is the crucial factor for the energy consumption in MANETs, we aim to maximize the interval between cluster messages while keeping the connectivity to the TA nodes at a sufficient level.

The third aspect illustrates the additional data overhead caused by the cluster algorithm. Since the amount of transmitted packets per second in our model can be simply calculated as "the number of nodes in the network divided by the frequency of cluster messages" and earlier measurements on the energy consumption of PDAs [21] have shown a considerable energy consumption of 40% for receiving (compared to sending) a packet, we examine the number of received packets as a metric for the data overhead.

Simulation 1: The first simulation, which models a platoon of soldiers traversing an urban area, is shown in figure 1. The figures 3 - 5 show the behavior of the network regarding to aspect 1) to 3) during the simulation for different cluster message frequencies of 2, 4 and 8 seconds.

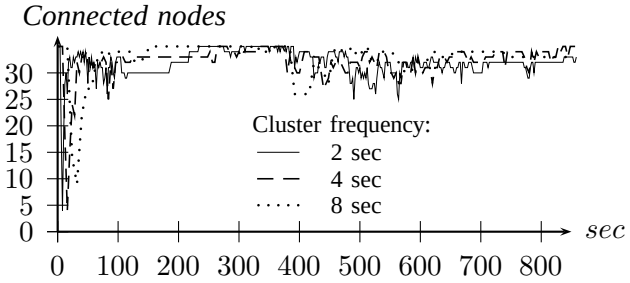

Fig. 3. Sim 1: Number of nodes connected to TA.

The initialization time as described in section III is set to 100 seconds. In this time the nodes are configured to choose their best TA connection node independent from

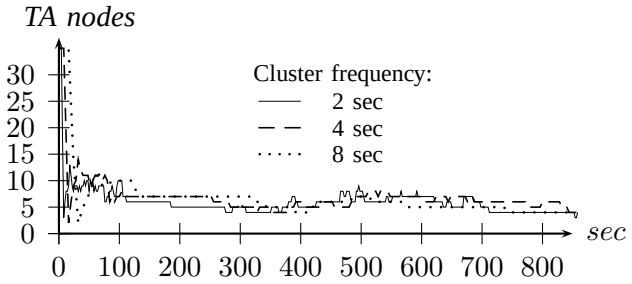

Fig. 4. Sim 1: Amount of TA nodes.

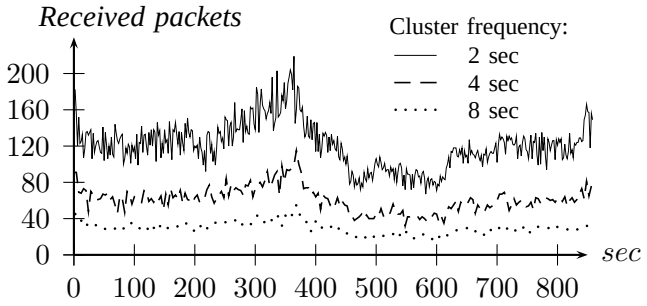

Fig. 5. Sim 1: Total number of received cluster packets/sec.

allready established TA nodes. After the initialization time, the reelection of TA members is encouraged to avoid too frequent changes of TA nodes (see section III). Figure 3 shows that directly after the start only 5 to 10 nodes are successfully connected to a TA node, while this number increases to more than 30 nodes after 20 to 80 seconds. The duration of this configuration process is dependent on the frequency of cluster messages. In the case of a cluster message frequency of 2 seconds (solid line) this process lasts only 20 seconds, while it takes 80 seconds in the case of a cluster frequency of 8 seconds (dotted line). According to this, the cluster algorithm needs approximately 10 rounds of cluster message exchanges to shape a sufficient set of TA nodes. In future work we will take advantage of this behavior and accelerate the initialization process by exchanging the first 10 cluster round messages in a short time period and fix this time as the initialization period.

After approximately 380 seconds (figure 1a)) the nodes start to split up between the buildings. The effect on the connectivity of the network and the TA can be seen in figure 3 and 5. The number of received packets increases until second 380, since the platoon needs to choose a closer formation to move in between the buildings. Thereupon this number decreases abruptly due to communication breakdowns. As an impact on the

connectivity to the TA in case of a 8 second cluster frequency (dotted line), up to 9 of the 35 nodes shortly loose their connection to the TA. In case of a cluster frequency of 2 (solid line) or 4 (dashed line) seconds the algorithm reacts quicker and only 5 nodes lose their connection to the TA.

A further crucial observation are the fluctuations in figure 3 between second 400 and 700 especially for a cluster frequency of 2 seconds (solid line). This behavior occurs, when the nodes from different small groups get a temporary connection between house walls, as can be identified in figure 1b). This problem does not occur for a cluster frequency of 8 seconds (dotted line) since the nodes of different small groups will not receive enough cluster messages to choose the new node from another group as TA node. In order to avoid this behavior, future work will investigate the increasing of the period `CONSTANT_CONNECTION_INTEREST` (section III) that a node needs to wait before effectively connecting to a new node.

Despite the fact that the number of received packets increases after the collation of the group (figure 1c), this event has no notable effect on the TA or the connectivity of the network. As a further important result of the figures 3 through 5 the cluster algorithm shows a very similar behavior for the different cluster message frequencies of 2, 4 and 8 seconds. In view of bootstrapping a security architecture on top of the TA, the consequence of this observation is that even in a network with numerous abrupt communication breakdowns, a cluster frequency of 8 or even more seconds is still sufficient.

Simulation 2: The second simulation models different movements techniques of a platoon of soldiers in a hostile area (figure 2). The figures 6 through 8 show the behavior of the network regarding to aspect 1) to 3) during the simulation for different cluster message frequencies of 4, 8 and 16 seconds. Additional simulations based on a message frequency of 8 seconds illustrating the influence of node failure, loose contacts of the wireless devices and different amounts of transmission power are shown in figure 9 through 11.

The behavior during the initialization time of 100 seconds is similar to simulation 1, where approximately 10 rounds of cluster message exchange are required to first shape a sufficient set of TA nodes (figure 6). Thereupon the number of received packets decreases due to the formation stretching of the traveling platoon during second 150 and 320 (figure 2a)). The partition in three squads which move in a compact formation till second 600 increases the number of received packets, while the

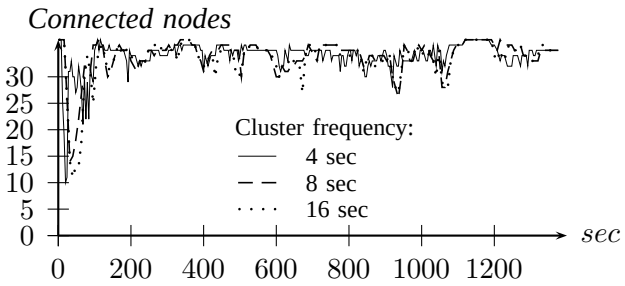

Fig. 6. Sim 2: Number of nodes connected to TA.

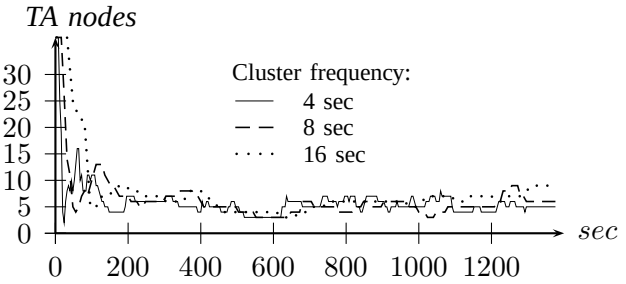

Fig. 7. Sim 2: Amount of TA nodes.

following formation change to a stretched line (figure 2b)) abruptly decreases this number. Nevertheless, these changes in the connectivity of the network have allmost no changes to the connectivity of the TA (figure 6) and the number of TA nodes (figure 7).

The only two noticeable events in the rest of the simulation that come with a short decrease of the connectivity to the TA are the resumption of speed after the file formation in figure 2b) and the division of the network in second 1070 (figure 2c)) while crossing the danger area. Recapitulating, the algorithm for the distribution of the TA works smoothly and does not show any weak points in this simulation scenario. For further refinement of the algorithm we have examined the influence of node failures, loose contacts and different amounts of transmission power as illustrated in the figures 9 through 11. The wireless devices of the nodes in the first of these scenarios begin to drop out during the enemy contact from second 700 to 800 (figure 2b)). A failure of 20 of the 37 nodes (dashed line in figure 9) exhibits almost no differences to a network without node failures (solid line). The first apparent influence can be observed in case of 25 failing nodes as illustrated by the dotted line.

We performed the same simulation scenario as illustrated in figure 9 a second time, while the wireless devices in this simulation only suffered from a loose

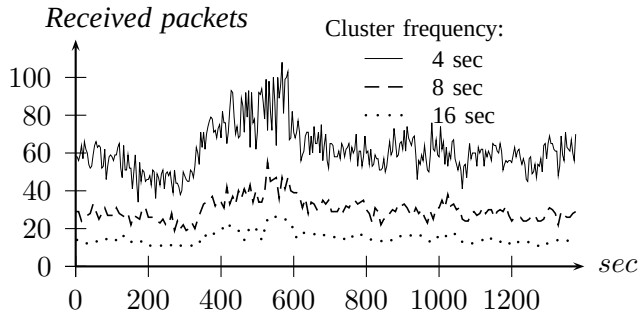

Fig. 8. Sim 2: Total number of received cluster packets/sec.

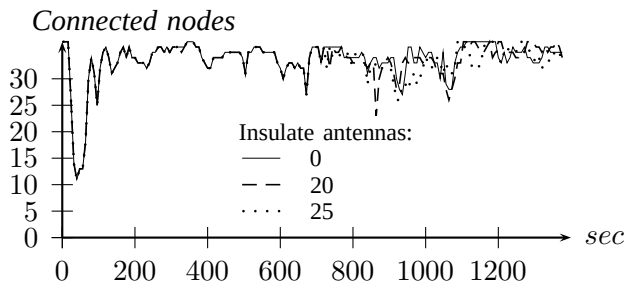

Fig. 10. Sim 2: Influence of loose contacts of several nodes on the number of nodes connected to TA. Cluster frequency: 8 sec.

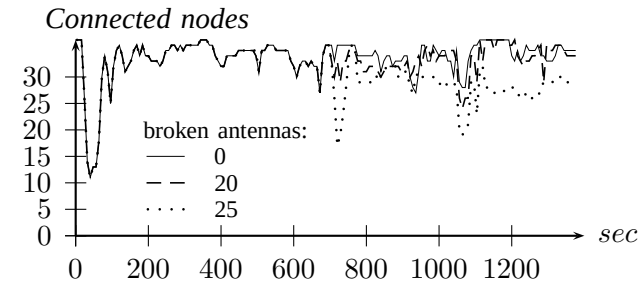

Fig. 9. Sim 2: Influence of the breakdown of several nodes on the number of nodes connected to TA. Cluster frequency: 8 sec.

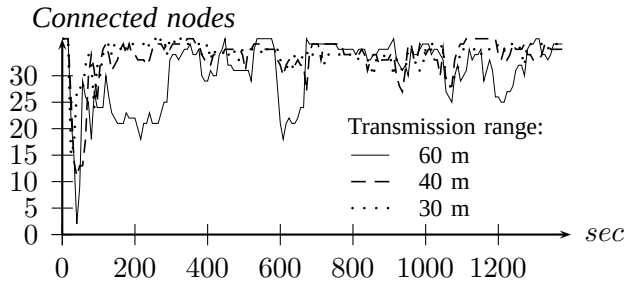

Fig. 11. Sim 2: Influence of different amounts of transmition power on the number of nodes connected to TA. Cluster frequency: 8 sec.

contact instead of failing totally. Loose contacts were simulated by a random failure in sending and receiving packets of 50% and the effected nodes were the same at the same time as in the former simulation. Even a number of 25 failing nodes have only minor impact on the connectivity to the TA, while a loose contact of 20 devices has no visible negative effect.

Finally we also ran the simulation 2 under different transmission strengths of 1mW, 5mW and 15mW yielding a communication range in free space of approximately 30, 45 and 60 metres, respectively. Our algorithm appeared to be sensitive to the stretching of the formation in case of a communication range of 60 metres (figure 11 solid line). During traveling in the period of 150 to 320 seconds, as well as after the division of the network after 600 seconds, the increasing distances between the nodes disconnect up to 15 nodes from the TA. This behavior occurs since a higher communication range enables the nodes to connect to far away TA members, that remove out of the connected nodes range at the mentioned events. In future work we will therefore configure the *quality value* of the cluster algorithm to encourage the choice of nearby nodes, i.e. set the loading of the signal strength metric as defined in [15] to a suitable value.

VI. Conclusion

In this paper we have extended and evaluated our cluster based algorithm for trust authority distribution in tactical mobile ad hoc networks. We put the main focus on a configuration yielding a suitably connected network, while producing as few as possible communication overhead. The two crucial points for the communication overhead are the number of changes of TA nodes and the frequency of the cluster algorithm messages. The issue of avoiding too frequent changes of TA members was addressed by our extension of the cluster algorithm in section III and the behavior of the algorithm for different cluster message frequencies was examined in section V. In order to evaluate our algorithm in realistic environments we prepared two simulation scenarios in which 35 and 37 nodes were moving in a platoon, splitting up between buildings and stretching the formation during faster marching, while single nodes suffered from broken or insulate wireless devices. The results of these simulations show, that the cluster message frequency in such scenarios can be chosen to 16 seconds or even longer and that the period between changes of TA members could be increased to 30 to 60 seconds (for cluster message frequency of 8 seconds) despite numerous formation changes during the simulations.

Future work will investigate a comfortably usuable group mobility model as well as a dynamic change of cluster frequency, e.g. more frequent cluster messages during the initialization or formation changes. In order to realize such a dynamic behavior, the TA overlay network will not only operate as a security architecture but also as a control unit for the underlying cluster algorithm. This control unit could for example prepare the network for an imminent devision by initiating an increase of the number of TA members and thus creating two or more operative TA overlays, one on every partition of the network. The results about the frequency of changes of the TA members and the connectivity to the TA prepare the basic parameters for bootstrapping this security architecture and control unit. Our research on a security architecture based on (k, n)-threshold cryptography will include traditional public key infrastructures as well as identity based public key cryptography, and evaluate methods for distributed computation.

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] 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*, Hongkong, March 2004.

[2] Tsai Lin-Jiun, Lin Jen-Chiun and Lai Feipei, "SWARM: Secure Wireless Ad-hoc network Reliance Management," in *Wireless Pervasive Computing, 2006*, 2006, pp. 1 – 6.

[3] Ueli Maurer, "Modelling a Public-Key Infrastructure," in *Proc. 1996 European Symposium on Research in Computer Security (ESORICS' 96)*, ser. Lecture Notes in Computer Science, E. Bertino, Ed., vol. 1146. Springer-Verlag, Sept. 1996, pp. 325 – 350.

[4] Michael K. Reiter and Stuart G. Stubblebine, "Authentication metric analysis and design," *ACM Transactions on Information and System Security (TISSEC)*, vol. 2, no. 2, pp. 138–158, May 1999. [Online]. Available: citeseer.ist.psu.edu/reiter99authentication.html

[5] G. Caronni, "Walking the Web of trust," in *IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'00)*. IEEE Computer Press,, 2000, pp. 153 – 158.

[6] Yan Lindsay Sun, Wei Yu, Zhu Han and K.J.Ray Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 305 – 317, Feb. 2006.

[7] G. Theodorakopoulos and J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, Feb. 2006.

[8] Carla-Fabiana Chiasserini, Imrich Chlamtac, Paolo Monti and Antonio Nucci, "An energy-efficient method for nodes assignment in cluster-based Ad Hoc networks," in *Wireless Networks*, vol. 10. Springer, May 2004.

[9] D.J. Baker and A. Ephremides, "The Architectural Organization of a Mobile Radio Network via a Distributed Algorithm," *IEEE Transactions on Communications*, vol. 29, pp. 1694 – 1701, 1981.

[10] D. Baker, A. Ephremides and J.A. Flynn, "The Design and Simulation of a Mobile Radio Network with Distributed Control," *IEEE Journal on Selected Areas in Communications*, vol. 2, pp. 226 – 237, 1984.

[11] Taek Jin Kwon and Mario Gerla, "Efficient flooding with Passive Clustering (PC) in ad hoc networks," in *ACM SIGCOMM. Computer Communication Review*, vol. 32. ACM Press, January 2002.

[12] Stefan Pleisch, Mahesh Balakrishnan, Ken Birman and Robbert van Renesse, "Routing and forwarding: MISTRAL:: Efficient flooding in mobile ad-hoc networks," in *Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing MobiHoc '06*. ACM Press, May 2006.

[13] Foroohar Foroozan and Kemal Tepe, "A high performance cluster-based broadcasting algorithm for wireless ad hoc networks based on a novel gateway selection approach," in *Proceedings of the 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks PE-WASUN '05*. ACM Press, October 2005.

[14] X.-Y. L. Yu Wang, WeiZhao Wang, "Distributed low-cost backbone formation for wireless ad hoc networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing MobiHoc '05*. ACM Press, May 2005.

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

[16] Alan D. Amis, Ravi Prakash, Dung Huynh and Thai Vuong, "Max-Min D-Cluster Formation in Wireless Ad Hoc Networks," in *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM '02*, 2000, pp. 32–41. [Online]. Available: citeseer.ist.psu.edu/amis00maxmin.html

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

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

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

[20] "Military Operations." [Online]. Available: http://www.globalsecurity.org/military/library/policy/army/fm/7-8/

[21] P. Gauthier, D. Harada and M. Stemm, "Reducing Power Consumption for the Next Generation of PDAs: It's in the Network Interface." [Online]. Available: citeseer.ist.psu.edu/10096.html