Best-Effort Data Leakage Prevention in Inter-Organizational Tactical MANETs

Johan Sigholm
Dept. of Military Studies
Swedish National Defence College
Stockholm, Sweden

Massimiliano Raciti
Dept. of Computer and Information Science
Linköping University
Linköping, Sweden

***Abstract*—Reconfigurable Radio Systems (RRS), based on Software Defined Radio (SDR) and Mobile Ad-hoc Network (MANET) technologies, offer considerable advantages for military operations, such as increased network survivability and interoperability. The RRS-based Common Tactical Radio System (GTRS), currently in development by the Swedish Armed Forces, is designed for use in diverse geographical settings and for purposes varying from international combat missions to national contingency operations. However, protecting these networks from attacks and safeguarding the carried information against leaks is an ongoing research challenge, especially in combined scenarios where tactical data may flow across organizational boundaries.**

This paper presents a best-effort approach to Data Leakage Prevention (DLP) for inter-organizational RRS-based networks. The proposed architecture makes use of data mining techniques and an efficient *n*-dimensional clustering algorithm which has previously been successfully used for real-time anomaly detection in critical infrastructure protection. The DLP architecture is developed as an extension to the GTRS system, modeled and simulated in OPNET™ Modeler. Our results show that common data leaks can be efficiently identified by the proposed scheme, while keeping the important false positive rate at a very low level.

Keywords—Mobile ad-hoc networks, data leakage prevention, information security, interoperability, military communications, M&S, OPNET

I. Introduction

When it comes to tactical communications, there is currently a significant change taking place within many armed forces around the world. Historically, battlefield communications relaying voice and data messages between warfighters and commanders has been relying on diverse collections of static, hardware-intensive and branch-specific radio systems. Although these systems are still in common use, they are many times in desperate need of modernization [1]. This holds especially true when it comes to new requirements such as global interoperability, brought on by an intensified engagement in multinational, comprehensive operations involving military, civilian and non-government resources from numerous countries [2]. Other important factors involve the increased demands for high-speed wireless data capabilities in support of tactical broadband networks and the time-sensitive targeting sensor-decider-shooter chain [3].

The change that is taking place, and that has actually been in the works since at least a couple of decades, is not an incremental step on the evolutionary map of wireless communications. It is rather a quite substantial leap, which involves the concept of liberating users of tactical radio systems from the bonds that hold them to one particular frequency or protocol for the duration of the radio hardware lifespan. The goal is instead a single, universal radio, capable of supporting everything from traditional voice communications to Internet browsing, high quality video conferencing, and information sharing with allied partners.

These next-generation tactical radio systems are sometimes referred to as Reconfigurable Radio Systems (RRS). They encompass several underlying technologies such as Software Defined Radio (SDR), Mobile Ad-hoc Networks (MANETs) and Cognitive Radio (CR). Research on these technologies has been extensive during the last decade, attracting substantial amounts of R&D resources, not least within the U.S. Joint Tactical Radio (JTRS) program. Among the greatest potentials that these new tactical systems show is being able to overcome problems of technical heterogeneity, while simultaneously offering improved network survivability in comparison to legacy systems [4]. But as promising as this development sounds, many challenges still need to be overcome. Remaining obstacles do not only relate to specific technical difficulties, but may in large parts be attributed to the rate of growth of overall system complexity. The lingering development problems, with accompanying runaway budgets, have led some critics to call the JTRS project “a blueprint for failing big” [5], whereas official explanations attribute the problems to poor understanding of the technical challenges of mobile ad-hoc networks due to the immaturity of the technology, contractor issues and information assurance requirements [6].

Concerns about information assurance in RRS-based networks is something has come into the focus of attention of the Common Tactical Radio System (GTRS) project, a joint tactical radio development program with close relations to JTRS, funded by the Swedish Armed Forces (SwAF). In a report written by a group of associated researchers at the Swedish Defence Research Agency (FOI) regarding IT security in GTRS, the authors assert that one of the main

problems with designing security solutions for a RRS is that it is at least one generation newer that the mental image of what a tactical communications system is supposed to resemble [7].

When working in collaborative environments, such as during combined missions or international disaster response, inter-organizational information and resource sharing is important for efficient asset use, yielding a comprehensive Common Operational Picture and allowing for accurate Blue Force Tracking [8], [9]. However, safeguarding sensitive or classified resources residing in the network requires security measures to prevent data loss as a result of various attacks. The broadcast nature of MANET communication makes these networks inherently difficult to secure, and problems such as a constantly changing network topology, and interference or jamming become additional challenges [4], [10]. Nevertheless, if the commutations system is perceived as too complicated by the end users, they may turn to other, less secure channels [7].

The contradicting demands of an easily accessible, but yet adequately secure, collaboration space require some method of data protection. Intrusion Detection Systems (IDS) have been in the spotlight for researchers during the last decade or so. However, due to the risk of malicious code gaining system access through out-of-band channels, e.g. piggybacking on an insecure USB drive, and the possibility of attacks initiated by authorized insiders, more attention has recently instead been put on preventing sensitive data from leaving the network, sometimes called extrusion detection or Data Leakage Prevention (DLP). DLP aims to take a holistic approach to data protection, including information residing in a computer system (data in use), information on network-attached storage systems (data at rest), and information leaving the organizational boundary via some communications protocol (data in motion). The concept has by some security experts been criticized for being inefficient or of dubious value at best [11], whereas others claim that DLP represents a significant contribution to information security, not only by stopping "stupid employees" from making mistakes, but also as a remedy to frequently changing organizational structures and the operational reality of many environments as shown by experience [12].

In this paper, our approach to DLP for a collaborative tactical scenario has been to focus on data in motion, i.e. information flowing across an organizational boundary. Our aim is to investigate how best-effort DLP can be achieved for an inter-organizational RRS, based on previous experience from anomaly detection in other environments. The goal of such a system is to minimize data loss, while simultaneously allowing a relatively open network for collaboration, and also taking resource constraints of individual nodes into count.

The paper is structured as follows; Section II presents related work previously done in the area. Section III describes the basics of the GTRS system, the anomaly detection algorithm ADWICE, and the proposed best-effort DLP architecture. Section IV presents the simulated scenario, and the results are offered in Section V. The paper ends with some concluding remarks in Section VI.

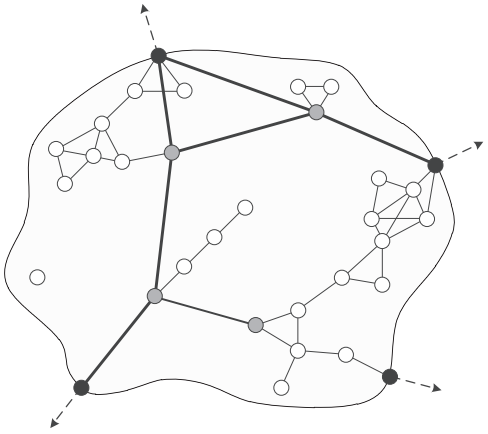

Fig. 1. Conceptual structure of a GTRS network

II. Related Work

Mobile ad-hoc networking has been a subject of intense research attention during the last decade. Apart from the development of protocols and architectures to improve network robustness, delay tolerance, throughput rates, routing performance etc., the dynamic nature of such networks has also raised the need of techniques for protecting them from various security threats. Several approaches to intrusion detection have been proposed during the years, ranging from simple and standalone architectures, where every node in the network works independently to discover anomalies, to hierarchical distributed solutions, where nodes collaborate to increase detection performance. For a broad overview of MANET security architectures, the reader is referred to the comprehensive surveys [13], [14] and [15].

Information assurance is an especially important issue in military scenarios, where a security breach could ultimately cost soldiers their lives. Although some recent research focus has been put on developing methods to secure tactical MANETs, the considered scenarios have commonly been homogeneous environments, where one military organization has full control over the communications equipment, and where initial device management and planning is an a priori requirement. The MITE project [16], sponsored by the German Armed Forces, includes a cluster-based anomaly detector, CBAD, that focuses on identifying misbehaving MANET nodes. Other approaches can be found in [17], where a host-based cross-layer IDS architecture is proposed, and in [18], where a biometric-enabled IDS is suggested in order to produce a high-security tactical MANET environment. Ensuring strict confidentiality has also been the focus of research funded by the SwAF so far, where the approach has been to enforce hard segmentation of the network into secure and insecure domains [19]. However, this approach does not address the need of achieving acceptable levels of security in the less secure network domains. In the context that this paper

is concerned with, i.e. a tactical environment where efficient inter-organizational collaboration is paramount, a rigorous mandatory security scheme is neither required nor possible to enforce. Moreover, rather than focusing on discovery of misbehaving entities, or the detection of malicious activity within the boundaries of the own organization, our aim is to limit possible data leaks within the cross-boundary data flows in a best-effort fashion.

III. Background

A. GTRS

The Common Tactical Radio System (GTRS) is the future mobile communications network for the Swedish Armed Forces (SwAF), currently under development. GTRS will form one of the cornerstones in the future joint C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) as the main data transmission system for the internal Service Oriented Architecture, offering functions and services for the SwAF, as well as providing a communications bridge to external parties such as allied forces or collaborating Non-Governmental Organizations (NGOs).

As part of an adopted Commercial off-the-shelf (COTS) defense acquisition strategy, Sweden's Defence Materiel Administration (FMV) has selected FlexNet™-Four Software Defined Radios (FN4) from Rockwell Collins, Inc. as a platform for SwAF GTRS ground mobile communications. The FN4 employs a Mobile Ad-hoc Networking (MANET) structure supporting a distributed system of mobile nodes that are autonomous and self-organizing.

A GTRS network consists of nodes that may be connected by several different waveforms. In Fig. 1 this is illustrated by clusters of white nodes connected with short-range wideband links, while the gray nodes (and most of the black nodes) also support a narrow-band low frequency waveform which allows for long-range connections. The black nodes act as border gateways to external networks, by either wireless or fixed-line connections. The GTRS network is based on a layered protocol architecture, with TCP/IP protocols running on top of the custom MAC and radio layers. The MANET-supporting lower protocol layers handle changes in link quality and loss or disappearance of intermediate nodes, intentional and unintentional RF interference, and multi-path effects created by the high mobility.

B. ADWICE

Anomaly Detection With fast Incremental Clustering (ADWICE) [20] is an anomaly detection scheme based on the BIRCH clustering algorithm [21]. It has previously been successfully used as a component in critical information infrastructure protection [22], as well as a means of detecting contaminants in drinking water [23]. Since anomaly detection is effective when searching for irregular patterns in large data sets, we have chosen ADWICE as the basis of our DLP approach. The basic concept of the algorithm is to take multi-dimensional vectors as input, containing characteristic features of each data sample, and grouping these vectors in clusters. For each cluster a condensed feature set (CF) is generated containing the n number of data points in the cluster, their linear sum (**S**), and the square sum of the data points (SS). From the CF of a cluster, the centroid v_0 and radius R is obtained by calculating:

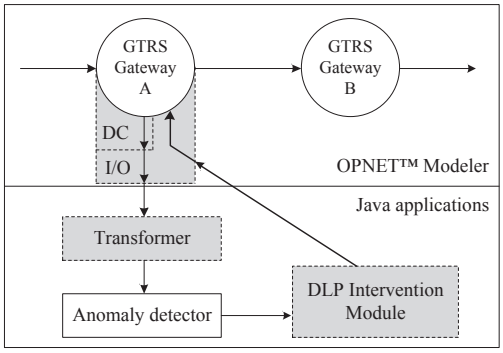

Fig. 2. The Best-effort DLP architecture

$$v_0 = \sum_{i=1}^{n} v_i / n \tag{1}$$

$$R(\mathrm{CF}) = \sqrt{\sum_{i=1}^{n} (v_i - v_0)^2 / n} \tag{2}$$

The distance between a new data point and a cluster is thus the Euclidian distance between the point and the cluster centroid. This is used to evaluate if a new data point is close enough to a cluster to be part of it, if it should form a new cluster during the training phase, or if it is an outlier (anomaly) in the detection phase.

Two clusters $CF_i = (n_i, \mathbf{S}_i, SS_i)$ and $CF_j = (n_j, \mathbf{S}_j, SS_j)$, or a cluster and a single data point, may be merged by computing $(n_i+n_j, \mathbf{S}_i+\mathbf{S}_j, SS_i+SS_j)$. In this way a new data point can make an incremental update to an existing cluster in an efficient way, which is important for speeding up the processing of input data indexing in the learning phase, but also when searching through clusters in the later detection phase.

In the training (or learning) phase, ADWICE creates a normality model by generating a set of clusters organized in a tree structure. Each level in the tree represents a summary of the clusters below by creating a new CF, which is the sum of the CFs in the lower branches. There are two parameters which need to be configured manually in order to optimize search efficiency for the given normality data set; the maximum number of clusters (M), that is used by the algorithm when creating the normality model, and a cluster centroid distance threshold (E), that is used when determining whether a new data point falls within its closest cluster or not.

The importance of performance and scalability of anomaly detection naturally depends on the application. Whereas anomaly detection in critical infrastructures may require real-time performance, slow processes with gradual change may benefit more from higher accuracy than minimal time-to-detection. The complexity of training and detection in ADWICE is linear to the input data, which stands in contrast to other clustering techniques than require quadratic time [22]. In addition, since ADWICE does not need the training data to be kept in main memory during training runs, its scalability characteristic is further improved as larger training models can be accommodated for.

C. *Best-effort DLP Architecture*

The proposed best-effort DLP architecture is illustrated in Fig. 2. The preexisting components are displayed in white, whereas our modifications are shown in gray with dotted lines. It consists of two parts, additions to the GTRS gateway radio model in the simulation environment, and two external Java applications. The radio model was extended with two modules, a data capture function (DC) which intercepts IP packets leaving the network, and an input/output function (I/O) for data exchange with the simulation environment.

The first added external application is a transformer module that is responsible for selecting the basic features of the input data and creating suitable output for the anomaly detector. In our implementation, the data from the simulation is transformed into numerical feature vectors to be used by our selected anomaly detector, ADWICE.

The second module is the DLP intervention module, which receives alarms from the anomaly detector, performs alarm aggregation, and sends feed-back back into the simulation environment in order to stop a detected data leak. We have discussed a possible solution with a mechanism that can terminate an ongoing leak in [4], but the actual implementation is left as future work. This could include centrally blacklisting misbehaving nodes in border gateways, distributed blacklisting throughout the MANET by use of gossip-style protocols, or using more aggressive methods like inserting specially crafted TCP RST (reset) messages which forces the connection that carries leaking data between two nodes to close on both sides.

IV. SIMULATIONS

The GTRS network is simulated in the OPNET™ Modeler network simulator [24] (see Fig. 3). FMV has provided us with custom models for the GTRS (FN4) radios, developed for the SwAF by Rockwell Collins. We also received specifications for various types of application traffic which may be generated in the network, including custom C4ISR traffic. Using our extensions described above, we can perform training of the anomaly detector by running a simulation where the network is running in "normal" mode. The normality model can then be used as a baseline for detecting

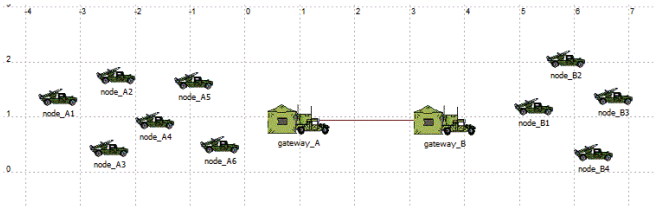

Fig. 3. Layout of the scenario simulated in OPNET™ modeler

TACTICAL APPLICATION PROFILE	TRANSPORT PROTOCOL
SwAF custom C4ISR	TCP + UDP
Voice communications	UDP
Video communications	UDP
Text-based communications	TCP
Database access	TCP
HTTP-based communications	TCP
Document printing	TCP

Table 1. Normal production traffic generated in the network

anomalies, which are created by generating traffic representing "data leaks" passing through the border gateway. The basic features that are selected to characterize the captured traffic are based on information in the transport and IP layer headers. Only TCP and UDP packets are captured, other traffic, such as network routing information, is discarded. The features are *source host*, *source port*, *destination host*, *destination port*, *transport protocol* (UDP or TCP), *headers* (compound attribute) and *message length*.

Choosing a suitable scenario for our simulations is a non-trivial task. Depending on how the nodes are positioned, how they move, where the organizational boundary is drawn, which nodes that may communicate with which, and what traffic that is transmitted over the network, the results may vary. After consulting experienced military communications specialists within the SwAF, we decided that a reasonable precondition is that traffic between two organizations is required to pass through an intermediary (border) gateway. This gateway may be stationary or mobile, and there could be several such border gateways, but application traffic should generally not be able to flow directly between two end nodes in two separate networks. In our implementation we chose a scenario with a single, static border gateway that the inter-organizational traffic must pass.

Another important component of building a realistic scenario is deciding what traffic should represent normality, and what should be considered to be anomalous. Normal traffic in our scenario was chosen from the standard traffic profiles that we had been provided with (see Table 1), flowing between the two organizations, A and B. The data leaks were represented by two custom created application profiles; "Leak Type 1", an encrypted point-to-point connection with ten times or more traffic outbound than inbound on average, and "Leak Type 2", an unencrypted FTP file transfer session, where groups of files averaging 500 kB in size where transferred off the network. Both normal and anomalous

traffic was transmitted between different nodes, with random intervals.

We ran a total of five one-hour simulations to generate normality model traces (NT) and another five simulations to generate verification traces (VT), including both normal traffic and some cases of anomalous data leaks. During verification, when computing the feature vector, we add a label with "0" if a packet is part of normal traffic, or with a "1" if it is part of a data leak, to be used as a reference when evaluating the outcome of the anomaly detection.

The performance of the anomaly detector is measured by two commonly used metrics, detection rate (DR) and false positive rate (FPR). DR measures the percentage of anomalies that are correctly classified, and is defined as:

$$DR = \frac{TP}{TP + FN} \tag{3}$$

In (3) TP refers to the number of true positives and FN refers to the number of false negatives. The false positive rate (FPR) is the percentage of normal data that is misclassified as anomalous, and is defined as:

$$FPR = \frac{FP}{FP + TN} \tag{4}$$

In (4) FP refers to the number of false positives and TN refers to the number of true negatives.

Our ambition was to get a detection rate (DR) which is as close to 1 as possible, while the false positive rate (FPR) should be as close to 0 as possible. Since we had a best-effort approach, a low FPR is preferred over a high DR.

As previously mentioned, ADWICE takes two parameters; a maximum number of clusters (M) and a cluster centroid distance threshold (E). Finding the optimal number of clusters for a given domain is a common data mining problem for clustering algorithms. The suitable number of clusters is normally dependent on the distribution and sparseness of data in the multidimensional space. For this reason, the maximum number of clusters has been experimentally determined by varying M in the range M={100,200,…,1000}.

The cluster centroid distance threshold (E) must also be determined to properly separate the clusters from the outliers. A small threshold tends to overfit the data, leading to a high FPR. A large threshold, on the other hand, leads to a low DR. To find the best combination of these values that fits the normality, one run was made for each setting of M={100,200,…,1000}, E={0.1,0.2,…,2.0}, NT={1,2,…,5}, and VT={1,2,…,5}. The exploration of the parameter space thus required a total of 5000 runs, taking about one week to execute on five parallel computers. This was done to find a configuration that yielded an acceptable trade-off between DR and FPR, to be used for real-time anomaly detection.

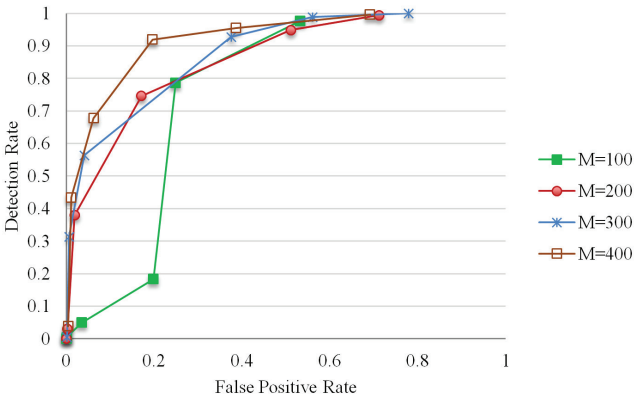

Fig. 4. ROC curves for M={100,…,400}

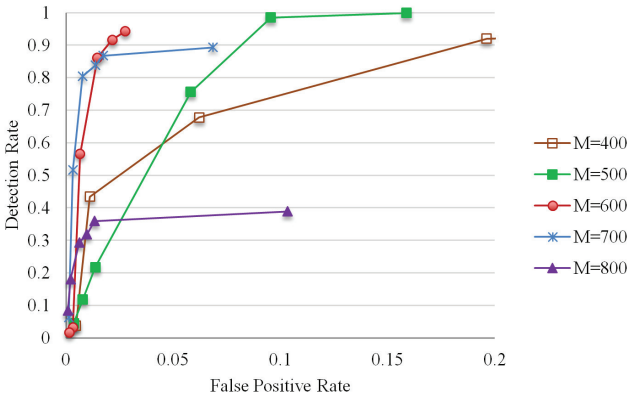

Fig. 5. ROC curves for M={400,…,800}

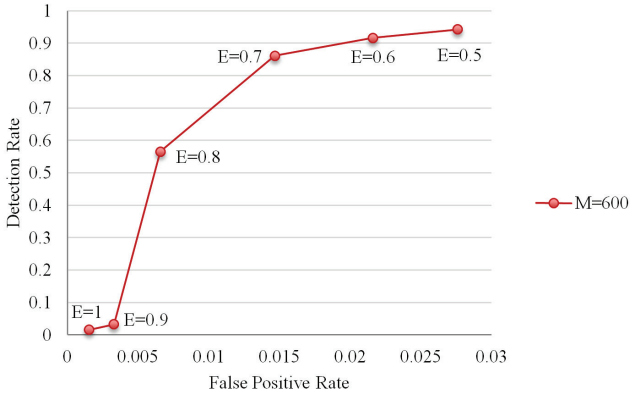

Fig. 6. ROC curve for M=600

V. Results

When evaluating the performance of our proposed architecture, the most interesting metric is the accuracy of the data leak detection algorithm. The results of the detection runs are illustrated in Fig. 4-6 above, with the detection rate (DR) on the Y-axis and the false positive rate (FPR) on the X-axis. This type of diagram is known from signal detection theory as the Receiver Operating Characteristic, or ROC curve. The region of interest in the graph is the top left quartile, where DR is high and FPR is low.

Figure 4 shows four ROC curves where M is increased from 100 to 400. For each curve the value of M is fixed and the data points correspond to values of DR and FPR obtained when fixing the threshold E. The six points on each curve in Fig. 4 correspond to six values of E in the range between 0.5 and 1 where useful results were obtained. As can be observed in the figure, better results are achieved as M is increased. For instance, when M=400 we obtained a 92 % detection rate at the cost of a 20 % false positive rate, or a 68 % detection rate at the cost of 6 % false positive rate, which would be more reasonable in our best-effort scenario.

In Fig. 5 we can see that when M is increased further, even better performance is observed. In fact, we can see the curves of M={500,600,700} are outperforming the case of M=400, which is repeated in Fig. 5 for comparison. However, when M is increased above 600, performance drops, and when M is at 800 we observe a drastic reduction of the detection rate. This can be understood by realizing that a too high number of clusters will tend to overfit the data points in the normality model, and a lower threshold would be required to avoid a high number of false negatives. In fact, the lower detection rate when M=800, and E is in the same range as before, is caused by a higher number of false negatives. Overfitting the model would also generate a higher number of false positives, as a new normal observation would be slightly more distant than any of the normality clusters. Another problem with having a high number of clusters is that it increases the model complexity, which has a performance impact in terms of longer search times in the cluster indexing structure.

Overall, the best results are achieved when M=600. In this case, as depicted in Fig. 6, we obtained a 94 % detection rate while the false positive rate remained below 3 %, by setting E to 0.5. An even lower FPR, 1.5 %, which would be preferable in our scenario, can be obtained by setting E to 0.7. This still gives us a reasonably high DR of 86 %.

VI. Conclusion

Our ambition in this paper was to design a best-effort Data Leakage Protection architecture for use in inter-organizational tactical MANETs. We have proposed such a solution, and implemented it as an extension of radio models in the OPNET™ simulation environment and as external Java modules interacting with the ADWICE anomaly detector. Our results show that anomaly detection can be used to identify data leaks in an inter-organizational network. In the selected scenario, we could limit the false positive rate to 1.5 %, while still achieving a detection rate of 86 %. We believe that these results are fully adequate for a best-effort strategy.

During the work with this paper we have identified several areas in which our architecture may be improved. We are currently analyzing how the DLP architecture performs when data leaks are divided over two or more separate GTRS border gateways. Further future work includes extending the architecture with a mechanism that can terminate an ongoing leak when discovered, and an interface to a trust authority system like the one described in [25]. The efficiency of the anomaly detector could be increased by adding more features in order to better characterize the nature of the traffic that is flowing between the networks, such as trends over longer time periods. Another possible future extension of the architecture is an addition of a misuse detection module, which more rapidly could detect leaks by use of signatures of known malicious patterns, or other advanced detection approaches as described in [26].

As always in anomaly detection, simulation results depend on how well the training data models actual normality. Although we believe that our selected scenario is reasonably realistic, the validity of our results could be reinforced by using real-world packet-capture data and movement trace files instead of generated data and a mobility model. We therefore plan to further evaluate the architecture using data from a military exercise or similar event.

Acknowledgment

This work was supported by funding from the Swedish Armed Forces Doctoral Program and the Swedish National Graduate School in Computer Science (CUGS). The authors would like to thank Kalle Burbeck and Simin Nadjm-Tehrani for offering access to the original ADWICE source code, and to Thorbjörn Ericson at the Swedish Defence Materiel Administration (FMV) for providing the custom GTRS radio models for OPNET™ Modeler.

References

[1] D. Axe, “Inside the army’s doomed quest for the ‘perfect’ radio,” *Wired Magazine*, Jan. 2012 [Online]. Available: http://www.wired.com/dangerroom/2012/01/army-perfect-radio/

[2] E. Törnqvist, J. Sigholm, and S. Nadjm-Tehrani, “Hastily formed networks for disaster response: Technical heterogeneity and virtual pockets of local order,” in *Proc. 6th Int. Conf. on Information Systems for Crisis Response and Management (ISCRAM2009)*, Gothenburg, Sweden, May 2009.

[3] L. Löfgren and J. Sigholm, “Military technology for resource-limited time-sensitive targeting,” in *Proc. 2010 Symposium on Military Sciences*, National Defence University, Helsinki, Finland, May 2010.

[4] J. Sigholm, “Reconfigurable radio systems: Towards secure collaboration for peace support and public safety,” in *Proc. 9th European Conference on Information Warfare and Security (ECIW 2010)*, Thessaloniki, Greece, Jul. 2010.

[5] S. Gallagher, “How to blow $6 billion on a tech project,” *Ars Technica*, Jun. 2012 [Online]. Available: http://arstechnica.com/information-technology/2012/06/how-to-blow-6-billion-on-a-tech-project/

[6] F. Kendall, Letter to the United States Congress pursuant to the termination of the JTRS GMR program, Oct. 2011 [Online]. Available: http://www.govexec.com/pdfs/101411bb1.pdf

[7] A. Hunstad, H. Karlzén, and J. Löfvenberg, “IT security in GRTS: Risk inventory and scenarios,” Technical Report FOI-R--2980--SE, Swedish Defence Research Agency, Linköping, Sweden, Apr. 2010.

[8] S. Rousseau, F. Benbadis, D. Lavaux, and V. Conan, "Public safety situation aware services over cognitive radio networks," in *Proc. 8th IEEE Int. Conf. on Mobile Ad-Hoc and Sensor Systems (MASS 2011)*, Valencia, Spain, Oct. 2011.

[9] R. E. Donnelly, "Impact of the network environment on a common operating environment," in *Proc. IEEE Military Communications Conf. 2011 (MILCOM 2011)*, Baltimore, MD, USA, Nov. 2011.

[10] F. Maxén, "A comparative analysis of network approaches for tactical wireless communications, validated by Joint Communication Simulation System (JCSS) simulations: A Swedish perspective," *Master's Thesis*, Naval Postgraduate School, Monterey, CA, USA, Sept. 2011.

[11] R. Bejtlich, "Data leakage protection thoughts," TaoSecurity, Feb. 2009 [Online]. Available: http://taosecurity.blogspot.com/2009/02/data-leakage-protection-thoughts.html

[12] K. Rowney, "Six myths of information security," Symantec Corp., Mar. 2009 [Online]. Available: http://www.symantec.com/connect/blogs/six-myths-information-security

[13] V. Pomponiu, "Securing wireless ad hoc networks: State of the art and challenges," in J. Zubairi and A. Mahboob (eds.), *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies* (pp. 1-22), IGI Global, Aug. 2011.

[14] C. Xenakis, C. Panos, and I. Stavrakakis, "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks," *Computers & Security*, vol. 30, no. 1, pp. 63-80, Jan. 2011.

[15] M. N. Lima, A. L. dos Santos, and G. Pujolle, "A survey of survivability in mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 66-77, Jan. 2009.

[16] M. Jahnke, A. Wenzel, G. Klein, N. Aschenbruck, E. Gerhards-Padilla, P. Ebinger, and S. Karsch, "MITE – MANET intrusion detection for tactical environments," in *Proc. NATO/RTO Research Symposium on Information Assurance for Emerging and Future Military Systems*, Ljubljana, Slovenia, Oct. 2008.

[17] R. Shrestha, K.-H. Han, D.-Y. Choi, and S.-J. Han, "A novel cross layer intrusion detection system in MANET," in *Proc. 24th IEEE Int. Conf. on Advanced Information Networking and Applications (AINA 2010)*, Perth, Australia, Apr. 2010.

[18] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," *IEEE Trans. on Wireless Communications*, vol. 10, no. 9, Sept. 2011.

[19] J. Grönkvist, A. Hansson, J. Nilsson, M. Sköld, and J. Svensson, "Multiple services in heterogeneous ad hoc networks," Technical Report FOI-R--2886--SE, Swedish Defence Research Agency, Linköping, Sweden, Dec. 2009.

[20] K. Burbeck and S. Nadjm-Tehrani, "ADWICE: Anomaly detection with real-time incremental clustering," in *Proc. 7th Int. Conf. on Inform. Security and Cryptology (ICISC 04)*, Seoul, Korea, Dec. 2004.

[21] T. Zhang, R. Ramakrishnan, and M. Livny, "BIRCH: An efficient data clustering method for very large databases," in *Proc. ACM Int. Conf. on Management of Data (SIGMOD)*, Montreal, Canada, Jun. 1996.

[22] K. Burbeck and S. Nadjm-Tehrani, "Adaptive real-time anomaly detection with incremental clustering," *Information Security Technical Report*, vol. 12, no. 1, Mar. 2007.

[23] M. Raciti, J. Cucurull, and S. Nadjm-Tehrani, "Anomaly detection in water management systems," in J. Lopez, R. Setola, and S. D. Wolthusen (eds.) *Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*, Lecture Notes in Computer Science (LNCS) vol. 7130, pp. 98-119, Springer-Verlag Berlin Heidelberg, Mar. 2012.

[24] OPNET Technologies, Inc., *OPNET Modeler®* [Online]. Available: http://www.opnet.com/

[25] S. Reidt and S. D. Wolthusen, "Efficient trust authority distribution in tactical MANET environments," in *Proc. IEEE Military Communications Conf. 2007 (MILCOM 2007)*, Orlando, FL, USA, Oct. 2007.

[26] R. Koch, "Towards next-generation intrusion detection," in *Proc. 3rd Int. Conf. on Cyber Conflict*, Tallinn, Estonia, Jun. 2011.