Assessment Simulation Model for Uncoupled Message Authentication

Laurin Doerr, Dalibor Fiala
University of West Bohemia
Pilsen, Czech Republic
laurind@kiv.zcu.cz, dalfia@kiv.zcu.cz

Michael Heigl, Martin Schramm
Deggendorf Institute of Technology
Deggendorf, Germany
michael.heigl@th-deg.de, martin.schramm@th-deg.de

***Abstract*—Today's trend of an increasing number of networked embedded devices pervades many areas. Ranging from home automation, industrial or automotive applications with a large number of different protocols, low resources and often high demands on real-time make it difficult to secure the communication of such systems. A concept of an uncoupled MAC which is able to ensure the authenticity and integrity of communication flows between two network parties can be used. This is in particular of advance for outdated legacy components still participating in the network. In this paper a assessment simulation model of the mechanism behind this technology is described. It outlines the probability of detecting an attack depending on the message authentication overhead. The model considers all control variables and performs measurements based on random data traffic. The results of the statistical analysis state that a high attack detection rate can be obtained even with a small communication overhead.**

I. Introduction

As the diversity of devices connected to each other steadily grows accompanied with a continuous rising of communication flows, network monitoring and traffic-based anomaly detection play a crucial role in future systems. In order to perform traffic monitoring and anomaly detection in networks with an increasing amount of traffic, sampling has become an essential mechanism meaning packets are measured and analyzed in a selective manner. SSDE, described in [1], encrypts only significant data of a message. [2] presents an encryption mechanism also based on selective data especially for image transmission. For transmitting time critical data, as in the case of many embedded systems, this can lead to a unstable system. If encryption or decryption fails, packets are not guaranteed to be delivered within its deterministic time window. Since confidentiality is often a minor priority in such networks, encryption can be neglected. A model using an intrusion detection system (IDS) based on selective packet sampling has been proposed in [3]. However, IDS in the embedded environment are associated with some drawbacks. Signature-based systems strongly depend on the protocol being used and anomaly based systems are mostly accompanied with a high false positive rate. For distributed IDS, the systems need to be small in terms of resource consumption but then lack a variety of features. A novel approach that counteracts the disadvantages is performing selective message authentication. The message authentication code (MAC) is not added to the normal data packets but is transmitted through a secure communication channel. This prevents failures through the MAC generation and does not delay the traffic. In [4] an embedded plug-in device is described which secures the data transmission through this mechanism without influencing the data flow using uncoupled MACs.

However, since sampled traffic is an incomplete approximation of the actual one, the question arises how reliable an intruder can be detected through the proposed algorithm. The proper adjustment of the variables involved in sampling packets is vital particularly with regard to effective management of the bandwidth.

The rest of this paper is structured as follows: Section II gives details on the system behaviour of the embedded plug-in device mechanism. The proposed assessment model is described in section III. Section IV deals with the results of the performed simulations. A short conclusion and a glance at the future work of the ongoing research work is finalizing the paper in section V.

II. System behaviour

Embedded plug-in devices inserted in the network provide authenticity and integrity for transmitted traffic. The technology has been introduced in [4] and was further developed in [5]. A simple network scenario is shown in figure 1 in which two end devices (A and B) are communicating with each other. For simplification reasons of the proposed assessment model, a sender device A is only sending packets ($m_{A\rightarrow B}$) to receiver B. The plug-in devices C and D ideally forward the network traffic with zero latency in order to keep the communication flows untouched. The main task of the plug-in devices is to generate and verify message authentication codes for the forwarded packets which are transferred uncoupled from the original ones. In the example C is generating a message authentication code $MAC(m_{A\rightarrow B})$ over packet $m_{A\rightarrow B}$ and is sending it to D. Plug-in device D forwarded the original packet, computed the message authentication code and stored it until $MAC(m_{A\rightarrow B})$ from C arrives for verification. Ideally, each packet should be measured and verified with a message authentication code in order to protect the communication flow. However, this would lead to a significant increase of the network traffic which is only possible in networks with low bandwidth utilization. In order to detect an attack in

ISBN 978-80-261-0642-5,

networks with low capacities it is not always necessary to observe the entire traffic. It is sufficient to measure only for a certain amount of time. This will divide the mechanism into multiple phases presented in [5]. The Setup Phase is used to establish a secure channel between two communicating plug-in devices, but will be neglected for the assessment of the actual uncoupled MAC algorithm. The Runtime Phase is split into two phases. During the Idle Phase which lasts a random time duration no measurements are performed which does not allow to detect an intruder Z for instance injecting malicious traffic to B ($m_{Z\to B}$). In contrast to the mechanism presented in [5] the plug-in devices negotiate during the Setup Phase which device acts as the master or slave. The master is then responsible to start a MAC Phase after the random time expired by informing the slave to generate and verify message authentication codes. This is done by sending a regulation packet that contains a random number of packets to be measured from device A. If a packet from device A is forwarded during the MAC Phase, plug-in device C is sending a generation packet to D containing the generated $MAC(m_{A\to B})$, a timestamp and a sequence counter for, e.g., replay attack protection. Using the proposed assessment model it is possible to determine how the parameters defining the MAC Phase need to be adjusted in order to detect an intruder at different bandwidth utilizations.

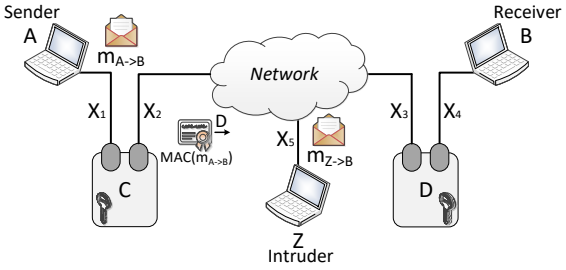

Fig. 1. Concept of the Embedded Plug-In Device

III. Assessment Model

For testing the probability of successfully detecting injected intruder packets with a different quantity of measured packets, a simulation model was developed using the programming language Python. Because the system behaviour of the plug-in devices is very complex, some simplifications had to be made. This includes that only one direction of transmitted packets is considered meaning A and Z are sending packets to B. Thus, also the communication of the plug-in devices is reduced in just sending regulation and generation packets from C to D. Feedback or heartbeat messages as presented in [5] are not considered in the model.

First, the sequence of the intruder detection by the plug-in device mechanism was abstracted. Figure 2 shows the modelled sequence of a measurement over a time period. There are two phases within a measurement cycle. Within the Idle Phase the next random measuring interval time is defined by determing a random number of packets that need to be authenticated. Subsequently, the MAC phase begins with securing the packets. As soon as the last sender packet has been captured, the next Idle Phase starts. No measurement or calculation takes place in this phase. An intruder has two ways to intervene the network traffic. He can either inject packets into the network or manipulate a packet sent by the transceiver A. Since only injecting packets affects the bandwidth, this case will be considered in the model.

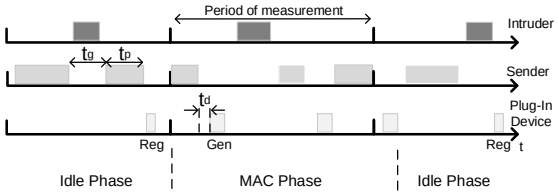

Fig. 2. Timeline of a Measurement Cycle

In order to make a statement about the used bandwidth, the associated link utilizations are calculated for each simulated traffic. The definition of the capacity of a link j and the used bandwidth are taken from [6]. Hence, the link usage of every simulation component can be calculated. The definition of available bandwidth is the unused part of the link capacity during a time interval. The used link capacity of a link $X_j = X_j(t, \Delta)$ is defined by

$$X_j = \frac{1}{\Delta} A_j[t - \Delta, t] \tag{1}$$

in which A_j is the cross traffic in bits over the link j during a time interval Δ.

A. Input and Control Variables of the Model

The model has several input variables. These are described in the following.

Global Parameters

- C: maximum link utilization of the transmission medium (10 mbps, 100 mbps or 1000 mbps for an Ethernet network)
- $tmax$: time window of a simulation in seconds
- Δ: computation time interval in seconds of one bandwidth measurement
- e: packet travelling time from plug-in device C to D
- t_d: delay time which a plug-in device needs in order to process and send out a generation packet delayed to the original sender packet
- $steps$: granularity of the simulation time window

Control Parameters

- $nmin, nmax$: Boundaries for the number of packets $n = ran(nmin, nmax)$ to be measured during a MAC Phase
- $alphamin, alphamax$: Boundaries for the waiting time $alpha = ran(alphamin, alphamax)$ defining the Idle Phase
- $tmingap\_A, tmaxgap\_A$: Boundaries for the time gap between each consecutive packet sent by A
- $min\_packet\_size\_A, max\_packet\_size\_A$: Boundaries for the size of each consecutive packet sent by A

- $tmingap\_Z, tmaxgap\_Z$: Boundaries for the time gap between each consecutive packet sent by Z
- $min\_packet\_size\_Z, max\_packet\_size\_Z$: Boundaries for the size of each consecutive packet sent by Z

B. Module Description of the Model

The model has been divided into six modules in order to easily adapt and extend the simulation. Figure 3 shows the interaction of the individual modules.

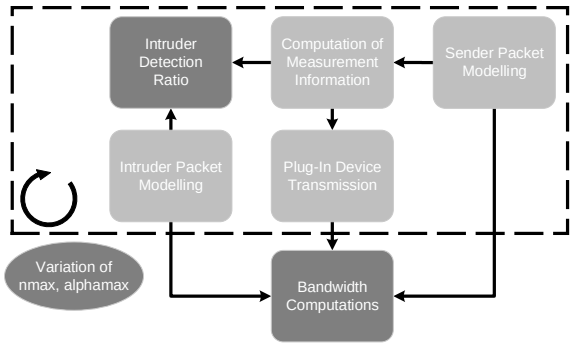

Fig. 3. Interaction of the Modules

1) Sender Packet Modelling: This module is used to simulate traffic from A to B. The packet flow is designed by a time gap between each consecutive packet and the size of each transmitted packet i. Both the time gap $t_{gAi} = rand(tmingap\_A, tmaxgap\_A)$ and the size $A_{Ai} = rand(min\_packet\_size\_A, max\_packet\_size\_A)$ are random values with fix boundaries. Packets are generated as long as the sum of the packet transmission time $t_{pAi} = \frac{A_{Ai}}{C}$ and the time gap for every packet is approximately the maximum simulation time (equation 2 with index A).

2) Intruder Packet Modelling: This module is used to simulate traffic from Z to B. The packet flow is designed by a time gap between each consecutive packet and the size of each transmitted packet i. Both the time gap $t_{gZi} = rand(tmingap\_Z, tmaxgap\_Z)$ and the size $A_{Zi} = rand(min\_packet\_size\_Z, max\_packet\_size\_Z)$ are random values with fix boundaries. Packets are generated as long as the sum of the packet transmission time $t_{pZi} = \frac{A_{Zi}}{C}$ and the time gap for every packet is approximately the maximum simulation time (equation 2 with index Z).

$$tmax \approx \sum_{i=0}^{N} t_{g\{A/Z\}i} + t_{p\{A/Z\}i} \qquad (2)$$

3) Computation of Measurement Information: This module is used to calculate the start of every MAC Phase and the number of packets which have to be authenticated during each cycle. Therefore the time duration for the Idle Phase represented by the value $alpha$ will be created randomly within the boundaries of $alphamin$ an $alphamax$. The number of packets to be captured and processed n during the measurement cycle is computed randomly within the boundaries $nmin$ and $nmax$. The start and duration of a MAC Phase depends on the packets sent by the sender which is considered in this module as well. The measurement phases are iterated until $tmax$ is reached. The information at which point in time measurements take place and how many packets are measured per cycle is stored.

4) Plug-in Device Transmission: The simulation model considers the transmission of regulation and generation packets of the plug-in device C in order to model the correct bandwidth usage within the system. Fore each measurement cycle start a reg_packet is created with the size reg_packet_size and will be sent to D. Every sender packet that is within a MAC Phase causes the generation of a gen_packet of size gen_packet_size. The measurement phases are iterated until $tmax$ is reached. The information at which point in time a regulation and generation packet, that will be sent by the plug-in device, is stored.

5) Intruder Detection Ratio: The intruder detection measurement is simulated within this module. The results from the previously presented modules serve as a basis. The module checks whether a sent packet of the intruder falls into a MAC Phase and is thus detected. It further computes the amount of intruder packets that could be detected over the entire time $tmax$ of the simulation.

6) Bandwidth Computations: The bandwidth computations module is used for calculating the used bandwidth of each link j from figure 1. The computation of the bandwidth is done using equation 1. X_1 represents the link utilization of the sender device A and X_2 the sum of the link load of the plug-in device C and X_1. Thus, the link utilization of C yields $X_2 - X_1$. The intruder utilizes the link with X_5. The resulting capacity of the link to the plug-in device D is $X_3 = X_2 + X_5$.

IV. Simulation Results

Two simulations for a time window of $tmax$ = 10 sec and a Δ of 0.1 sec have been performed to assess the presented model. Simulation 1 considers the detection rate for different $alphamax$ and changing $nmax$. Simulation 2 examines the link utilizations and thus the plug-in device communication overhead for a chosen $nmax$ and $alphamax$ in order to get a detection rate of approximately 90 %.

A. Detection Rate in Relation to $nmax$ and $alphamax$

The listed parameters below have been used for simulation 1. Again they are set to obtain an average sender bandwidth load of approximately 50 % and an average intruder link capacity of roughly 20 %. Multiple measurements have been performed for one curve in figure 4 in which $nmax$ is iterating with a fix value for $alphamax$.

- $nmin$ = 0
- $nmax$ = 1500
- $nmax\_iterate\_step$ = 100
- $alphamin$ = 0
- $alphamax$ = 0.07 sec
- $alphamax\_iterate\_step$ = 0.02

In figure 4 the curves of simulation 1 with different $alphamax$ are illustrated. All curves aspire a final value for the detection rate depending on the value set for $alphamax$. The smaller the Idle Phase represented by $alphamax$ the higher the maximum value for the detection rate. Parameters can be obtained from this exponential approximation curves in order to obtain a desired detection rate.

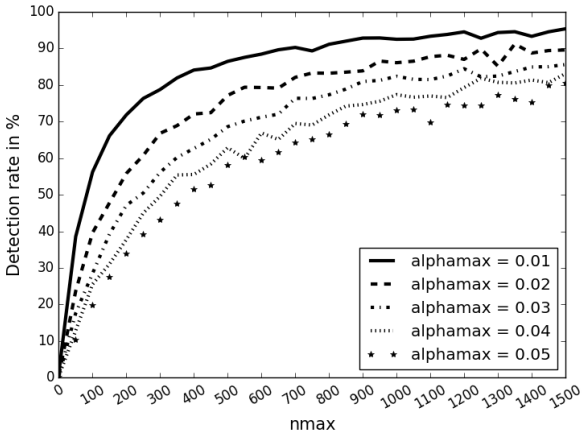

Fig. 4. Detection Rate over $nmax$ for Varying $alphamax$

B. Bandwidth Utilizations

The listed parameters below have been used for simulation 2. The sender and intruder parameters are set to obtain an average sender bandwidth load of approximately 50 % and an average intruder link capacity of roughly 20 %. The values for $alphamax$ and $nmax$ are taken from the graph of simulation 1 in order to obtain a detection rate of approximately 90%. The resulting bandwidth utilizations should ascertain how much additional traffic the plug-in devices are causing.

- $nmin$ = 0
- $nmax$ = 700
- $alphamin$ = 0
- $alphamax$ = 0.01 sec

In figure 5 the results of simulation 2 are illustrated. The curves represent the different link utilizations X_j. At a detection rate of 90.15 % an additional link load of only 6.56 % on average is generated by the plug-in device.

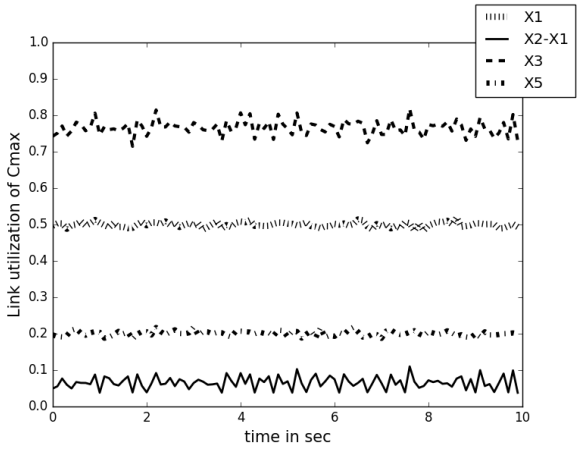

Fig. 5. Bandwidth utilizations with 90.15 % detection rate

V. Conclusion and Future Work

As the simulations have shown, the model can be used to determine the probability of the detection rate of an attack in which an intruder injects packets to a device. It can be determined how well an intruder can be detected at a given network load and maximum data overhead for the presented uncoupled MAC algorithm. Since the transmitted regulation and generation packets by the plug-in device are quite small in terms of their size, the resulting overhead bandwidth utilization mainly depends on the length of the Idle Phase defined through the $alphamax$ parameter. Thus, a reliable detection of an intrusion can be achieved even for a small communication overhead of the plug-in devices.

The proposed model is limited to a sender and a receiver device. In a real network more devices are participating the network. Therefore, the simulation model needs to be extended so that the network loud overhead caused by the uncoupled MAC algorithm and the detection rates can be examined with multiple sender, receiver and intruder devices. A simulation can be also performed through a virtual network based on [7] which relies on a Monte Carlo search tree. The advantage of such a virtual network would be the possible connection to a physical network environment for further tests of the uncoupled MAC algorithm.

Furthermore, the ongoing research work includes the substitution of the randomly generated sender and intruder traffic by a more precise simulation. It is planned to generate network packets on the basis of the network simulator ns-3 [8]. The simulation should be processed with a customizable random distribution to simulate different network and intruder behaviours.

Acknowledgment

This research work has been supported by the research projects no. 03FH016IA5 and 16KIS0539 of the German Federal Ministry of Education and Research and by the Ministry of Education, Youth and Sports of the Czech Republic under grant No. LO1506.

References

[1] Kushwaha, A., Sharma, H., Ambhaikar, A., *A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network*, 7th International Conference on Communication, Computing and Virtualization, 2016

[2] Spinsante, S., Gambi, E., *Selective encryption for efficient and secure transmission of compressed space images*, International Workshop on Satellite and Space Communications, 2009

[3] Bakhoum, E., *Intrusion detection model based on selective packet sampling*, EURASIP JIS, 2011

[4] Heigl, M., Schramm, M., Doerr, L., Grzemba, A., *Embedded Plug-In Devices to Secure Industrial Network Communications*, IEEE Applied Electronics, 2016

[5] Heigl, M., Aman, M., Fuchs, A., Grzemba, A., *Securing Industrial Legacy System Communication Through Interconnected Embedded Plug-In Devices*, Applied Research Conference (ARC), 2016

[6] Eklin, S., Nilsson, M., Hartikainen, E., *Real-Time Measurement of End-to-End Available Bandwidth using Kalman Filtering*, IEEE/IFIP NOMS, 2006

[7] Haeri, S., Trajkovi, L., *Virtual Network Embedding via Monte Carlo Tree Search*, IEEE Transactions on Cybernetics, 2017

[8] Agrawal, P., Vutukuru, M., *Trace based application layer modeling in ns-3*, Twenty Second National Conference on Communication (NCC), 2016