Czech Technical University in Prague

Doctoral Thesis Statement

Czech Technical University in Prague

Faculty of Electrical Engineering

Department of Telecommunication Engineering

Ing. Bc. Matěj Rohlík

Broadcast Security in Future Mobile Networks

Ph.D. Programme: Electrical Engineering and Information Technology

Branch of study: Telecommunication Engineering

Doctoral thesis statement for obtaining the academic title of "Doctor",
abbreviated to "Ph.D."

Prague, June 2012

The doctoral thesis was produced in combined manner

Ph.D. study at the department of Telecommunication Engineering of the Faculty of Electrical Engineering of the CTU in Prague

Candidate:	**Ing. Bc. Matěj Rohlík**
Establishment	Faculty of Electrical Engineering of the CTU in Prague
Address	Technická 2, 166 27 Prague 6
Supervisor:	**Ing. Tomáš Vaněk, Ph.D.**
Department	Department of Telecommunication Engineering Faculty of Electrical Engineering of the CTU in Prague Technická 2, 166 27 Prague 6

Opponents:

The doctoral thesis statement was distributed on:

The defence of the doctoral thesis will be held on....... at .... a.m./p.m. before the Board for the Defence of the Doctoral Thesis in the branch of study Telecommunication Engineering in the meeting room No. .... of the Faculty of Electrical Engineering of the CTU in Prague.

Those interested may get acquainted with the doctoral thesis concerned at the Dean Office of the Faculty of Electrical Engineering of the CTU in Prague, at the Department for Science and Research, Technická 2, Praha 6.

....

Chairman of the Board for the Defence of the Doctoral Thesis
in the branch of study Telecommunication Engineering
Faculty of Electrical Engineering of the CTU in Prague
Technická 2, 166 27 Prague 6.

Contents

1 Related Works

Any device connected to the global Internet network is continuously exposed to various types of threats. Very frequently, viruses, worms and malicious attacks jeopardise home as well as business devices [1]. However, appliances in non-Internet based networks are endangered as well. For instance, sensor networks, which are located in premises of a specific company and which are not connected to the Internet, can become a target of several damaging network attacks, where DoS is the most malicious type of attack. The comprehensive taxonomy of possible cyber-attacks is discussed in [2].

Due to these threats, an active approach to security is very important in the terms of data encryption, key distribution complex systems, authentication, authorisation, and accounting. A typical broadcast authentication communication within information systems is characterised by plain text communication between nodes, which do not mutually authenticate. Consequently, this represents the possibility where an attacker can theoretically reach the whole group of receivers with a malicious intention. To provide the respective access control key distribution, transmissions sources authentication, and streams non-repudiation, broadcast authentication protocols were designed. Even though there is a slight difference in the terms broadcast and multicast definition, the common attribute is that there always exist a group of receivers, no matter the amount of group members is equal to all or only a few members of the network. From the technical perspective, the communication is one-to-many or many-to-many [3].

Although the key management schemes are designed to exchange keys within group members to protect the traffic from different types of network attacks, they are not ready to cope with malicious network threats as the denial of service (DoS) type attacks. In [4], the authors analysed sensor network layers (as per ISO/OSI model) and possible DoS defences and confirmed that the limited resources of nodes make digital-signature schemes impractical and authentication poses serious difficulties.

Broadcast authentication is an essential service in distributed sensor networks. Because of the large number of sensor nodes and the broadcast nature of wireless communication, it is usually desirable for the base stations to broadcast commands and data to the sensor nodes. The authenticity of such commands and data is critical for the normal operation of sensor networks. Due to the resource constraints on sensor nodes and possible node compromises, broadcast authentication in wireless sensor networks is by no means a trivial problem [5].

In an unicast environment, the data authentication can be achieved using an elementary mechanism, where the transmitter and the message recipient share a secret (symmetric) key to compute a message authentication code (MAC). This cryptographic primitive assures the recipient that the transmitter generated the received message. Unfortunately, the common symmetric authentication method does not work in broadcast environment, because every recipient of the given message can impersonate the sender and forge the message, as the MAC key of the source transmitter is known to these nodes. Therefore, an asymmetric algorithm based on digital signatures is necessary for such purpose [6]. Thus, there exist two methods how to authenticate a broadcast transmission in sensor networks. The first way is to utilise a modified symmetric cryptographic algorithm and the second way is to apply an asymmetric cryptographic algorithm.

In broadcast networks, it is necessary to authenticate a single transmitter to more than one receiver [7]. The first possible solution is a hop-by-hop authentication of every message. Unfortunately, once a huge amount of messages approaches a specific node (e.g., a DoS attack situation), the authentication of every packet brings a huge delay from the end-to-end perspective [8]. None of the currently applied broadcast security protocols in sensor networks does effectively deal with DoS type attacks and does not minimise the end-to-end delay to prevent the overall energy depletion. Since this research work provides enhanced framework based on DREAM approach.

The DoS type of incident in the broadcasting communication can be prevented by verifying each packet's origin in the network. However, this method can influence and increase the time that the packets spent in the network and result into an almost impossible communication. This issue can be resolved by using the DoS resistant efficient authentication mechanism (DREAM) [9].

Besides DoS, the DDoS attack represents a more malicious threat. The DREAM mitigates the DDoS impact by involving analogous approach, where more stations are involved in the verification process. The DREAM can operate in two modes: normal and secure. In the secure mode, every incoming message is authenticated by the network node before being sent to the outgoing interface, whereas in the normal mode, some of the messages are sent directly to the outgoing interface without being authenticated. This approach mitigates a potential single point of failure in the whole network since there is not a single dedicated node where the authentication occurs, but distributed among the neighbours. The protocol functionality is influenced by the following parameters [10]:

- HT – number of nodes that message passed without authentication. For such each node, the parameter is incremented by one. When the packet is authenticated, HT is set to zero.
- NBR – number of neighbours.
- K – maximum number of nodes, that can message pass without authentication.
- b – expected number of neighbours in unity distance from the source.
- c – expected number of neighbours in unity distance from the last node that forwards the message.

The amount of messages to be sent or verified before sending out the interface is defined by the following decision rules (formulae):

$$Rand > \frac{b}{NBR}, \tag{1.1}$$

$$Rand > \frac{2 \cdot c}{NBR}, \tag{1.2}$$

where $Rand$ is a random number generated by every node for every message in the range of 0 and 1 with the uniform distribution. The node decides to authenticate/forward the message according to the (1.1) formula result, when the packet comes directly from a neighbour, the neighbour has been verified, or the parameter $HT = 0$. The node decides to authenticate/forward the message as per the (1.2) formula, in case the message did not come from a direct neighbour, the neighbour has not been verified, or the parameter $HT > 0$.

The emphasis on minimal energy consumption is common as well as the security and DoS resistance for both designs, the sensor networks as well as for femtocells [11, 12, 13]. The femtocell is a wireless network located indoors sharing the licensed wireless spectrum with the macrocell and is connected through a backhaul link, based on the well known Internet protocol (IP), to the mobile operator core network. Unlike the optimised deployment of macrocell base stations, the femtocell access points are very low-power and small base stations designed for the use in small spaces such as residential end-user households or small business environments without any supervision of the macrocell [14].

Compared to cellular systems, wireless local area networks (WLANs) had the primary purpose as an local area network (LAN) extension for those users, who cannot use the fixed wired connection. The 2G, 3G, and 4G cellular systems operate with a dedicated backbone and its network is usually separated from the Internet. The system as a whole is independent and fully functional without the global network. Nevertheless, the demand for IP services from mobile users caused mobile operators to extend their services and interconnect the mobile network with the Internet. These services enabled a new approach to reach uncovered indoor spaces with mobile signal by femtocells [15, 16, 17].

To ensure the availability and appropriate delay for sensitive traffic (packets carrying voice, signalling, real-time streaming voice/video data, etc.), the IP backhaul should assure quality of service (QoS) and provide appropriate security methods. That means the backhaul connection should provide enough capacity and parameters to avoid affecting the quality of voice call or carried data [18] and efficiently secure the communication as well.

The security aspects of FAP communication were part of the FREEDOM project [19]. Even though, several security models have been recently proposed, the security is currently a critical and unsolved challenge of cloud technology which requires to be standardised. The emerging technology enables to deliver computing as a service, commonly known as the cloud computing. The current femtocells provide only an interface between the mobile operator network and user mobile device via the IP-based network (Internet). Therefore, the femtocell technology provides a new environment for brand new mobile services development [20, 21].

Assuming the physical devices, network topology, and software are hidden from the user's perspective. Such deployment introduces a network cloud in the femtocell environment. As discussed in the previous paragraph, this is a brand new approach and does not have its generally accepted technical term. To distinguish the current femtocell from the above described approach, it is designated as the next generation femtocell (NGF) in this work[1].

The next generation femtocell deployment example, which is considered as the new future mobile technology is depicted in Fig. 1-1. The FAPs are commonly connected to the mobile operator network via secured tunnels to the femto security gateway (FSG). However, the FAPs are interconnected and enabled to communicate among them as well (direct FAP-to-FAP connectivity). The FAPs do have connectivity to respective resources (data storages, database servers, and other servers) based on the service offered by the mobile operator [23].

From the previous discussion can be seen that the sensor and future mobile environments address the same security, energy consumption, and parameter

[1] The authors in [22] use the NGF term in a more general way as they consider it as the future techology but they do not discuss any specific options nor the cloud feature at all.

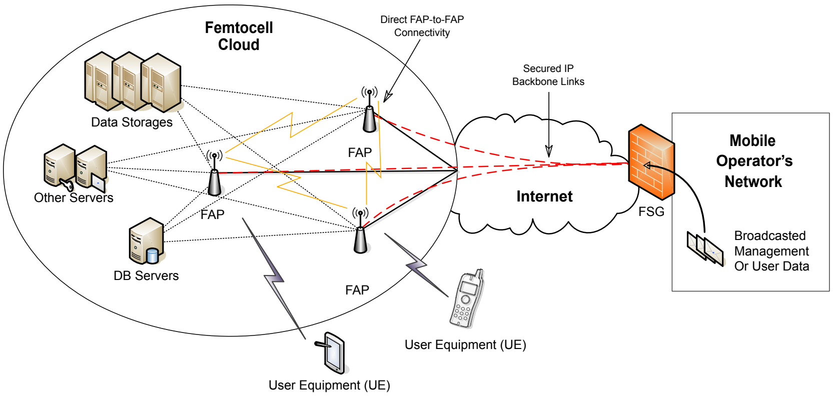

Femtocell Cloud
Direct FAP-to-FAP Connectivity
Secured IP Backbone Links
Data Storages
FAP
Other Servers
FAP
Internet
FSG
Mobile Operator's Network
Broadcasted Management Or User Data
DB Servers
FAP
User Equipment (UE)
User Equipment (UE)

Figure 1-1: The Next Generation Femtocell Deployment

requirements. Therefore, this thesis introduces a possible DREAM-based method how to deal with security (mainly DoS resistance), minimise end-to-end delay of valid messages, and save computing time (decrease energy consumption) by optimising the architecture of the DREAM.

2 Aim of the Dissertation Thesis

Mobile technology develops very fast as well as data services provided via mobile data networks. As the network devices can also be a target of a wide range of network security threats, the appropriate security methods are necessary to be implemented for protection. The most malicious is the denial of service attack, which can overload the appliances and prevent the mission-critical data from delivery. In the broadcast environment, which can be represented by future (next-generation) femtocell and cloud technology, the delivery becomes a significant challenge.

Since the broadcast authentication protocols and femtocell security belong to the areas of the author's interest, this dissertation thesis introduces a new scheme based on DoS Resistant Efficient Authentication Mechanism [9] with end-to-end delay and energy enhancements and applicable in future mobile (femtocell) environment [24, 3]. Despite the DREAM was originally designed to minimise end-to-end delay in broadcast networks, several parameters will be further examined and optimised based on the specific network conditions.

Based on the former research accomplished in the previously mentioned topics, the following goals of the dissertation thesis were determined:

- Design a new low latency DoS resistant mechanism for message authentication (IDARED) based on the DREAM scheme.
- The modification consists of:
  - involve split verification queue,
  - provide appropriate parameters selection,
  - reduce the total number of parameters of the mechanism.
- The new protocol should provide lower end-to-end delay compared to the DREAM mechanism.
- The proposed mechanism will be examined theoretically and simulated in MATLAB® environment.

3 Working Methods

To evaluate the DREAM behaviour, it was necessary to prepare an appropriate environment for simulations. Usually, the basic stochastic parameters, which are essential to correspondingly describe the examined scheme, are obtained from real network simulations. Despite the fact that the financial and space resources were limited, a basic simulation environment was developed to gather specific parameters of the DREAM behaviour to simulate the new protocol enhancements instead of the real world simulation.

As the main target of the research is to evaluate the DREAM behaviour, minimise the delay caused by the mechanism itself, and to be able to compare it with the newly proposed scheme, it was necessary to examine the stochastic distribution of its parameters. Therefore, the following assumptions were considered:

a) For simplicity, the links between each two nodes of the network are equal length, delay, and priority (cost).

b) As a consequence of a), a message can travel only one hop each round of the program.

c) The energy sources and computing power of nodes are constrained (wireless sensor network nodes and mobile femtocell access points are considered). Thus, all steps are treated to minimise energy requirements.

d) The public key signature verification is a relatively time consuming process (usually, in hundreds of milliseconds or seconds and depending on the overhead of lower layer protocols) and the power source of each node is limited (see c)). The duration of the previously described verification process was set as the referential value and denoted as a unit time delay (UTD). The UTD characterises the mean service time of the message verification process of each node.

e) For simplicity, parallel processing of tasks in the verification queue is not considered. Only a single message is processed at a moment as the spare CPU resources are served for other tasks.

In other words, since the UTD is platform dependent, the following definition clarifies that:

$$\begin{aligned} UTD &= 1 \\ &\text{or} \\ UTD &= 100\,[\%] \end{aligned} \tag{3.1}$$

represents the time required by the DREAM internal mechanism to process the verification procedure for a single message. Using the described approach, the research simulations provide hardware independent results, which are applicable for any platform of a specific device (network node) [25]. The original parameters, however, depend on the topology. The influence is caused by the average number of neighbouring nodes and its statistical dispersion.

The program (script) developed within this research has the following features. It simulates message broadcast propagation over a specified network [26]. The network structure can be determined manually by the user or generated randomly according to the Erdős-Rényi model [27], the Barabási-Albert model [28], the grid topology, and the N-ary tree structure.

The result of the previously described procedure is a square and symmetric matrix (the graph is undirected since messages can flow both directions) and having zeros on the main diagonal (no loops are allowed in the graph, because a node will not broadcast a message to itself). The simulation considers only non-weighted edges having the weight equal to one. The approach of saving details of every message may not seem to be system memory effective. However, it enables to track and evaluate all the sent/dropped messages after the simulation and the influence of the mechanism parameters and the stochastic distribution.

To be able to compare the results of simulations, a topology of specific parameters needs to be defined. The network topology, selected by the authors in [9] and [5], was set as a grid structure (Scenario 1) composed of 400 nodes, where 20 nodes were equally spaced in the grid in each row and column[2].

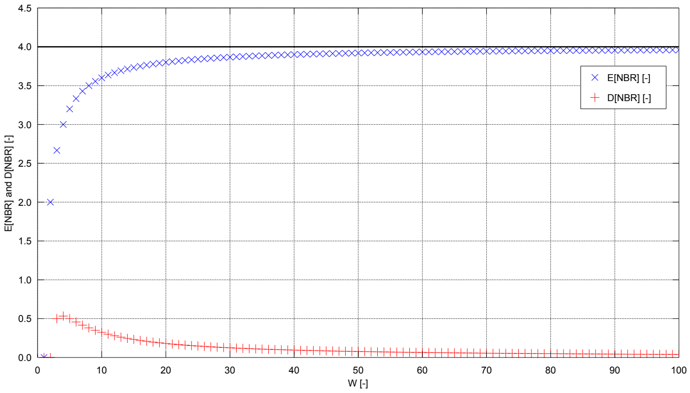


Figure 3-1: Average Number of Neighbours in WxW Grid Topology

Assuming the Scenario 1, increasing the width W of the grid network to infinity (the total number of nodes $N = W^2$), the average number of neighbouring nodes $\mathbb{E}[NBR]$ will converge to 4, since the number of nodes having three neighbours (nodes on the edges of the topology) and two neighbours (nodes in the four corners) is negligible compared to the total number of nodes Fig. 3-1. As per formula (3.2), the rest of the nodes will have number of neighbours equal to four. As per formula (3.3), the dispersion $\mathbb{D}[NBR]$ converges to zero.

$$\mathbb{E}[NBR] = \lim_{W\to\infty} \mathbb{E}[NBR(W)] = \lim_{W\to\infty} \left(-\frac{4}{W} + 4\right) \to 4, \tag{3.2}$$

$$\mathbb{D}[NBR] = \lim_{W\to\infty} \mathbb{D}[NBR(W)] \to 0, \tag{3.3}$$

$$\text{where } W = \{1, 2, 3, ...\} \tag{3.4}$$

To describe the DREAM using the respective mathematical model, it was necessary to examine the distribution of the HT parameter based on the K parameter setup.

[2] Assuming, the network graph $G = (V, E)$ is composed of a set of vertexes (nodes) $V = v_1, v_2, \ldots, v_N$, where $N = 1, 2, 3, ...$ is the number of nodes in G, and set of links (edges) $E = \{e_{ij}\}$, where $e_{ij} = \{v_i, v_j\}$ denotes an edge between vertex v_i and v_j, then two connected nodes are called adjacent and the degree k of a given node is the number of edges connecting it with other nodes ($k = deg(v)$), the mean of k over V is known as the mean degree $< k >$. As technically, the mean degree represents an average number of neighbours of the specific node $\mathbb{E}[NBR]$, the terminology will use the $\mathbb{E}[NBR]$ notation in this thesis [29].

The purpose of the K parameter is to limit the spread of unauthenticated messages through the network. In networks, where the $\mathbb{D}[NBR(W)] << \mathbb{E}[NBR]$ (here $\mathbb{E}[NBR] = 3.8$ and $\mathbb{D}[NBR] = 0.18045$), the distribution of HT in the network is naturally limited by a specific value of the K parameter, and its increasing values do not affect the distribution of HT. To preserve the equal chance a message can be authenticated before been sent and a message can be sent without prior authentication, the b and c parameters were set up to enable a 50% probability a message will be forwarded without prior verification and a 50% probability a message will be authenticated prior forwarding (see formulae (3.5) and (3.6)).

$$0 < b < NBR \quad \Rightarrow \quad b = \frac{NBR}{2} \tag{3.5}$$

$$0 < c < NBR/2 \quad \Rightarrow \quad c = \frac{NBR}{4} \tag{3.6}$$

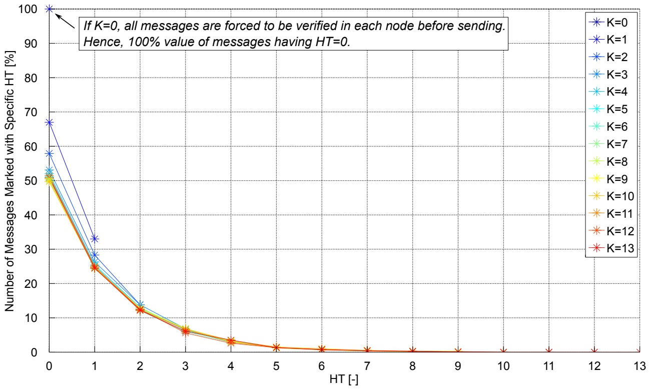


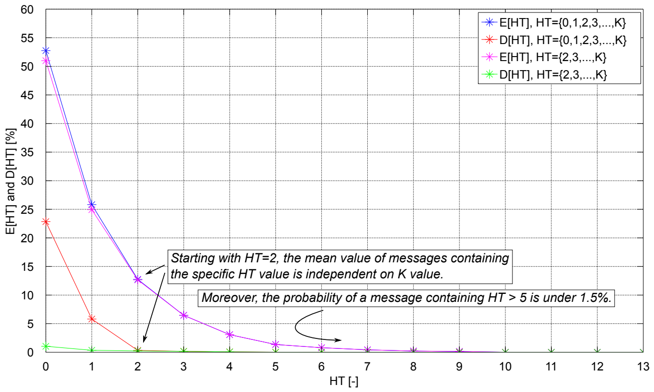
Figure 3-2: Influence of K On HT Distribution (Scenario 1)

The simulation of Scenario 1, where the transmitter was randomly chosen (uniform distribution) sending a single message throughout the network each iteration[3], was iterated 10^6 times and provided the following results:

- If $K = 0$, all messages are forced to be authenticated (hop-by-hop), i.e., 100% of messages has HT set to zero.
- If $K = 1$ or $K = 2$, the number of messages forced to be authenticated decreases approximately to 60%.
- If $K \geq 3$, the number of messages forced to be authenticated stabilises at 50%.
- Moreover, number of messages having $HT > 5$ was approximately under one percent. Therefore, choosing $K > 5$ does not affect the results, as the probability of appearance of such message is approximately 1%.

The simulation confirmed that, in a network composed of 400 nodes arranged as per Scenario 1, fifty percent of messages is being forced to be authenticated and fifty percent of messages is forwarded without prior verification, if $K \geq 3$ (see Fig. 3-2). Moreover, it does not have any effect to set $K > 5$ as the number of messages having $HT > 5$ is under one percent (see Fig. 3-3).

[3] A single iteration consists of broadcasting a message from a single node to all nodes in the network. Once the message is processed by the last node a new iteration is triggered.



Starting with HT=2, the mean value of messages containing the specific HT value is independent on K value.

Moreover, the probability of a message containing HT > 5 is under 1.5%.

Figure 3-3: Influence of K on Mean & Dispersion Values of HT (Scenario 1)

To examine the discussed parameters in a random topology, the simulation was accomplished for the selected random networks to compare them with the second scenario tested by the authors in [9] and [5], which was a random topology of 400 nodes. Unfortunately, the authors did not clarify the details and brought some confusion into the results of the accomplished experiment. Especially for the random network, the average number of nodes and dispersion of the average number of nodes were not provided, as it was significant and affects the mean end-to-end results and distribution of HT values in messages (the behaviour of the mechanism). All doubts and email reply from one of the authors is summarised in Appendix in the Doctoral Thesis fulltext. As the random topology details could not be obtained to design exactly the same scenario, only the Scenario 1 topology was taken into account for comparison with the new proposed authentication scheme.

The previously described simulations provided different distribution results of the HT values. Therefore, it was necessary to utilise some network topology oriented parameters to provide an appropriate mathematical model of the DREAM node (if such model exists) and to demonstrate the comparison results with the new proposed scheme, since the DREAM behaviour is strictly dependent on the network topology and its parameters.

$$D(G) = D_i = D_1, D_2, ..., D_N; \text{ where } D_1 \geq D_2 \geq \cdots \geq D_N \tag{3.7}$$

The authors in [30] introduced a specific approach how to measure homogeneity or heterogeneity of a given network. The method is based on the entropy of a degree sequence EDS examination. Assuming a graph $G(V, E)$ (see footnote[2]on page 6), N is the number of nodes, and $D(G)$ is the vector of degrees of nodes (see formula (3.7)).

The EDS as a new measure of the heterogeneity of complex networks and $NEDS$ represents a normalised entropy of degree sequence $NEDS$. The EDS can be calculated as per equation (3.8).

$$EDS = \frac{-\sum\limits_{i=1}^{N} D_i \ln D_i}{\sum\limits_{i=1}^{N} D_i} + \ln \sum_{i=1}^{N} D_i \tag{3.8}$$

As the $NEDS$ is defined as per equation (3.9), the results are normalised to $[0, 1]$ interval[4].

$$NEDS = \frac{EDS_{max} - EDS}{EDS_{max} - EDS_{min}} \tag{3.9}$$

The two random graphs were generated (according to scale-free – BA model and random ER model). A specific topology called N-ary tree, which represents a regular tree topology, where each node contains N child-nodes, was simulated as it is a scheme utilised for multicast networks [31]. The grid, as per Scenario 1, was examined as well, and a bus, star and full mesh topology were generated for reference. All simulated networks consisted of 400 nodes[5]. The results confirmed that the normalised entropy of degree sequence $NEDS$ corresponds to the variance of degrees of nodes $\mathbb{D}[Deg]$[6] (see Fig. 3-4).

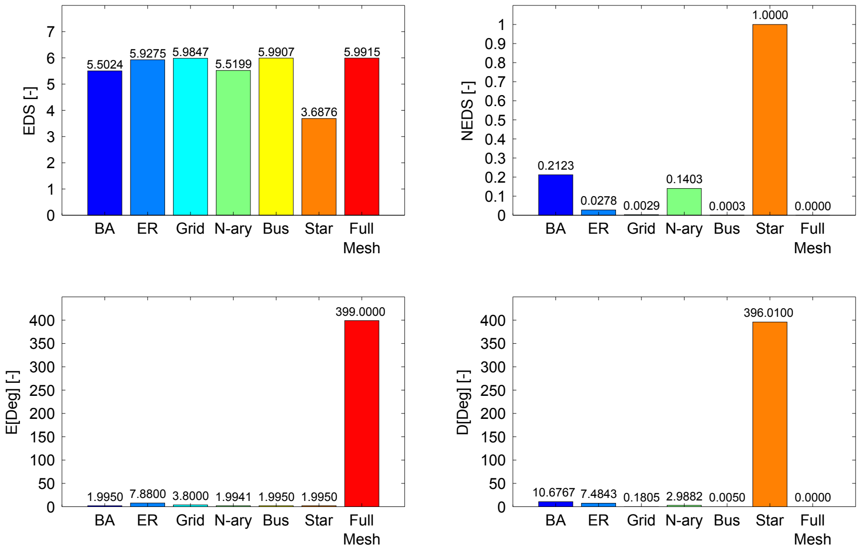


Figure 3-4: Results of Heterogeneity of the Selected Networks

The degree distribution of random networks were generated using the Barabási–Albert and Erdős–Rényi models. As discussed, the N-ary tree topology is used in broadcast networks. Thus, the degree distribution of such scheme was examined. Because the number of end nodes, forming the base of the hypothetical "network pyramid", is relatively large (due to the number of child nodes and length of the network), the group of single neighbour nodes dominates the degree distribution. For comparison purpose, the regular lattice[7] network (as per Scenario 1) confirmed that over 80% of nodes do have four neighbours and none has a single neighbour.

[4] Since the $D_i > 0$ and D_i is an integer, the minimum value of $EDS_{min} = (\ln 4(N-1))/2$. The maximum value of EDS corresponds to the most homogeneous (regular) network, and the minimum to the most heterogeneous (star) network [30].

[5] Only the N-ary tree consists of 341 nodes, as it is not possible to create an exactly 400 nodes network. The N-ary topology is based on 4 children nodes of each node and network length (depth) equal to four. It was compared with the respective 341-nodes full mesh network.

[6] Technically, the degree of a node represents the number of its neighbours.

[7] Regular or lattice network represent the same topology as the grid network.

As stated earlier, the random topology details are not specified in [9]. Therefore, to compare the results of the DREAM and the new proposed authentication scheme, only the Scenario 1 topology results was taken into account.

To approximate the DREAM using a mathematical model, it was necessary to define appropriate stochastic parameters. As these parameters of input data traffic and service times were not determined by the authors in [9], the input flow characteristics and the service time of the model were estimated as exponential. The exponential character was chosen with respect to the known formulae to calculate sojourn times, which enabled to express the measure of efficiency. The model is depicted in Fig. 3-5.

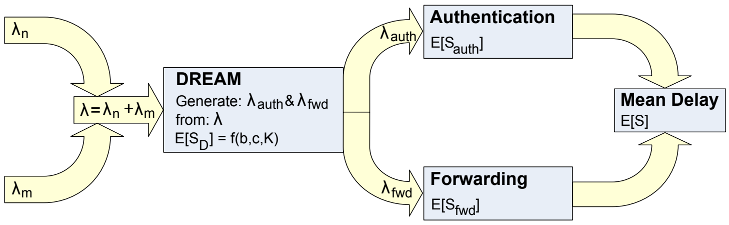


Figure 3-5: Mathematical Model of DREAM

Let the normal user data arrival rate is denoted as λ_n and the malicious user data arrival rate as λ_m. The two types of arrival rates produce the total arrival intensity λ, which is offered to the DREAM block, see formula (3.10).

$$\lambda = \lambda_n + \lambda_m \tag{3.10}$$

Based on the DREAM process, two different rates of customers are produced. The arrival rate of messages, determined to be authenticated prior forwarding, is denoted as λ_{auth} and rate of messages, which were determined to be forwarded prior authentication, is denoted as λ_{fwd}.

Parameter	λ_n	λ_m	μ_D	μ_{auth}	μ_{fwd}
Value	0.5	1.0	10	2	10

Table 3-1: Derived DREAM Model Parameters

To be able to compare the results of both models, the previously discussed parameters were derived from [9] and are introduced in Tab. 3-1. The distribution of arrival rates and the service times were estimated as exponential, thus the M|M|1 model was utilised. As a result, the whole system consists of two series systems, the DREAM block and a system of a parallel block combination. Assuming the estimated exponential distribution of arrival rates and the service times [32, 33] the mean sojourn time of the whole complex model $\mathbb{E}[S]$ can be expressed as per the formula (3.11).

$$\mathbb{E}[S] = \mathbb{E}[S_D] + \mathbb{E}[S_{fj}] = \frac{1}{\mu_D - \lambda_D} + \frac{12 - \dfrac{\lambda_{auth} + \lambda_{fwd}}{\mu_{auth} + \mu_{fwd}}}{8} \cdot \frac{\dfrac{\lambda_{auth} + \lambda_{fwd}}{\mu_{auth} + \mu_{fwd}}}{1 - \dfrac{\lambda_{auth} + \lambda_{fwd}}{\mu_{auth} + \mu_{fwd}}} . \tag{3.11}$$

The simulation results, the usage conditions, the optimisation details of the mathematical model, which is the new protocol based on, and the selected results are introduced in the next section.

4 Selected Results

This section deals with selected results of the accomplished simulations. Based on these results, the usage conditions of the proposed model are discussed. The optimisation details and the new proposed latency efficient DoS resistant authentication mechanism IDARED are introduced. As the power efficiency of newly designed solutions is an important feature of contemporary solutions, the efficiency of energy sources utilisation estimation is outlined. However, the specific optimisation measure was not provided in this case and the limitations were clarified accordingly. Both schemes, the DREAM and the IDARED are confronted with respect to the end-to-end delay and security perspective.

Based on the probability decision (formulae (1.1) and (1.2)), the DREAM produces two flows of messages – the first flow of messages to be authenticated and the second flow to be forwarded prior sending out the outgoing interface. The probability a message will be authenticated prior forwarding P_{auth} can be obtained, when the number of authenticated messages is divided by the total amount of messages. Analogically, the P_{fwd} can be obtained. Thus, the validity of formula (4.1) is apparent.

$$P_{\mathrm{auth}} = 1 - P_{\mathrm{fwd}} \tag{4.1}$$

Reference data, to compare the proposed model results, were obtained from [9]. The arrival and service rates were estimated as exponential, and the mean sojourn time expressed as per formula (3.11). Although, the λ offered to the network node is known (see equation (3.10)), the DREAM produces two flows of messages. Messages to be delivered to the authentication queue λ_{auth} and messages to be forwarded λ_{fwd} (see Fig. 3-5). Basically, this process depends on parameters b, c, and K.

$$P_{\mathrm{fwd}} = p_1 \cdot p_2 \cdot \ldots \cdot p_{\mathrm{NHR}} = p^{\mathrm{NHR}}, \text{ where } p_1 = p_2 = \ldots = p_{\mathrm{NHR}} = p. \tag{4.2}$$

Assuming, that the forwarding probability p is the same in each hop (from the transmitter to the last node to receive the message) and the number of hops in a row is NHR, the probability P_{fwd} a message will be forwarded after passing NHR hops can be determined as per formula (4.2).

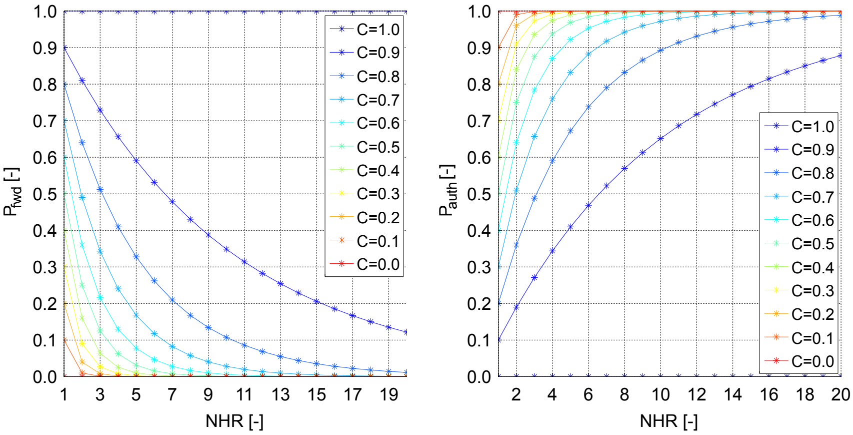


Figure 4-1: Message Authentication Probability

Although the existence of an unauthenticated message can be limited by the K parameter, the probability a message can travel several hops in a row without being verified is mainly determined by the C (and B) [8] parameter, as the applicable range of values of the K parameter is strictly limited by the B and C parameters. For instance, it is not beneficial to set the $K > 5$ (if $C = 0.5$) as the probability, a message will travel five or more hops, is below one percent (the bigger the K, the nearer to zero), and this is negligible from both, the security and the end to end delay perspective. Assuming, the K parameter represents the number of hops in a row a message can travel without authentication ($K = \text{NHR}$), the respective limit values of the K parameter can be calculated analogically (see results for selected values of C Fig. 4-1).

For a comparison purpose, the simulations were accomplished again for the specific case, where $b = c$. The results confirmed that the examined probabilities are mainly influenced by the b and c parameters and the influence of the K parameter was negligible (see Fig. 4-2).

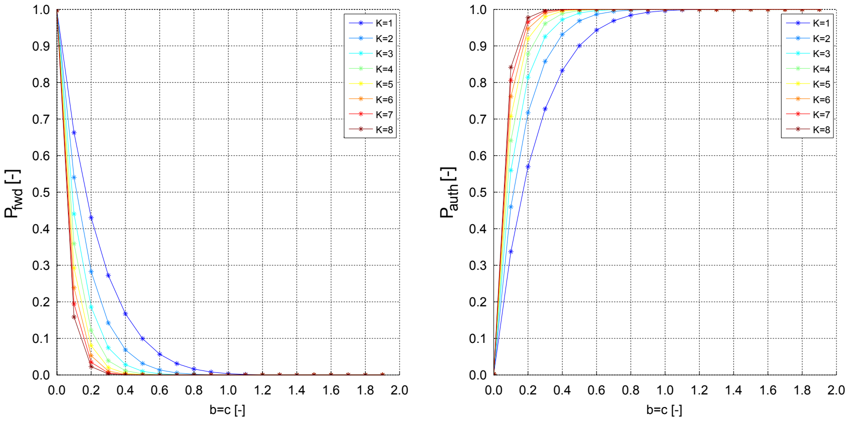


Figure 4-2: Influence of the K Parameter on Message Authentication Probability

The negligible influence of K parameter in Scenario 1 topology was also experimentally proved and clarified as per Fig. 3-2 and Fig. 3-3. The results represent a specific case where $C = 0.5$ (the normalised c parameter). Therefore, the K parameter will not be considered in the mathematical model.

The authors of the DREAM proposed b and c parameters to control the random mechanism behaviour. Once a message is received directly from a neighbouring node, the DREAM uses the b parameter. The c parameter is used in the rest of the nodes to affect the authenticate-first to forward-first ratio. Let the frequency of nodes, in which the b parameter is chosen (direct neighbours of the original transmitter), is denoted as f_b. The frequency of nodes, in which the c parameter is chosen, is denoted as f_c, and the BC_{ratio} is defined as per formula (4.3).

$$BC_{\text{ratio}} = \frac{f_b}{f_c} \tag{4.3}$$

The simulation was iterated 10^6 times and the following assumptions were considered. Four different networks (Scenario 1, random BA and ER models, and N-ary tree) were composed of 400 nodes [5], where each iteration produced a single message broadcasted from a randomly generated node (uniform distribution), and provided the following results. The BC_{ratio} is under one percent in random BA, grid

[8] These are the normalised b and c parameters which are discussed further. See formulae (4.5) and (4.6).

(Scenario 1), and N-ary network. And it is under two percent in random network generated using ER model (see Tab. 4-1).

10^6 iterations	Grid	ER	BA	N-ary
$\mathbb{E}[BC_{\text{ratio}}]$ [-]	0.0096	0.0016	0.005	0.006
$\mathbb{D}[BC_{\text{ratio}}]$ [-]	0.0001	0.0005	0.001	0.003

Table 4-1: Comparison of BC_{ratio} in Selected Networks

The probability a message will be authenticated (and forwarded) can be estimated, as the relative frequency of utilisation of both parameters, which were examined in the relatively high amount of iterations. To be able to express the P_{auth} dependence on b and c parameters, the relative frequencies f_b and f_c were taken into account. Assuming the relatively high amount of iterations, the relative frequencies were considered as equal to the respective probabilities $p_b \to f_b$ and $p_c \to f_c$ of influence of the specific parameter. This behaviour was addressed by the application of a weighted arithmetic mean as per equation (4.4)

$$P_{\text{auth}} = \frac{p_b \cdot B + p_c \cdot C}{p_b + p_c}\,, \tag{4.4}$$

where B and C are normalised b and c parameters as per equations (4.5) and (4.6). The maximum values are apparent from formulae (3.5) and (3.6), and likewise, it is obvious, that b is used to increase the authentication probability in the "one hop node" distance from the transmitter, and such probability is twice higher than for c.

$$B = 1 - \frac{b}{b_{max}} = 1 - \frac{b}{NBR} \tag{4.5}$$

$$C = 1 - \frac{c}{c_{max}} = 1 - \frac{2 \cdot c}{NBR} \tag{4.6}$$

The course of P_{auth} was examined as a function of both the b parameter and the c parameter. However, as per the original paper [9], the results were highlighted for a special case, where $b = c$, for further comparison.

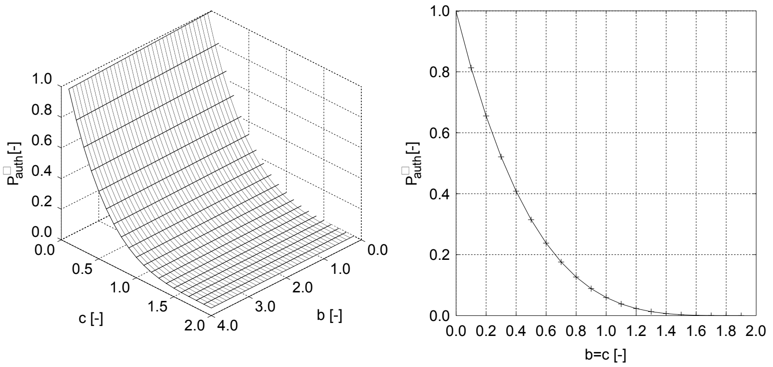


Figure 4-3: Influence of Parameters on Authentication Probability

Generally, the geometric character of the P_{auth} dependence is a plane, as the b and c parameters represent the corresponding limit, which is compared with the pseudorandom number. To address the utilisation factors of both parameters in real networks, the weighted arithmetic mean was applied at first. Since the previous step is independent on the network topology (assuming the 400 nodes topology), several approximation tests were accomplished to minimise the difference between the theoretical and real physical network topology (Scenario 1). The result is $P^{\square}_{\text{auth}}$ corresponding to the grid network represented by formula (4.7) and exponential dependency (see Fig. 4-3).

$$P^{\square}_{\text{auth}} = \text{EDS} \cdot (P_{\text{auth}})^{\text{NBR}}, \tag{4.7}$$

where EDS is the entropy of degree sequence and NBR is the mean number of neighbours (both related to Scenario 1). The complete $P^{\square}_{\text{auth}}$ is as per (4.8).

$$P^{\square}_{\text{auth}} = \text{EDS} \cdot \left(\frac{p_b \cdot \left(1 - \frac{b}{NBR}\right) + p_c \cdot \left(1 - \frac{2 \cdot c}{NBR}\right)}{p_b + p_c} \right)^{\text{NBR}} \tag{4.8}$$

The proposed model behaviour (the course of $\mathbb{E}[S]$) was studied under normal conditions ($\lambda = \lambda_n; \lambda_m = 0$) as well as in case a network device is being flooded by a huge amount of messages (under attack, $\lambda = \lambda_n + \lambda_m$). The simulated results were compared with the reference results published in [9]. The specific values of λ parameters were presented earlier in Tab. 3-1. The difference between the proposed model and the reference values increases with the decreasing value of the c parameter. The difference is above 2% for $c < 0.4$ and for approximately $c > 0.4$, the difference is below 2%, which was considered as an acceptable tolerance (see Fig. 4-4).

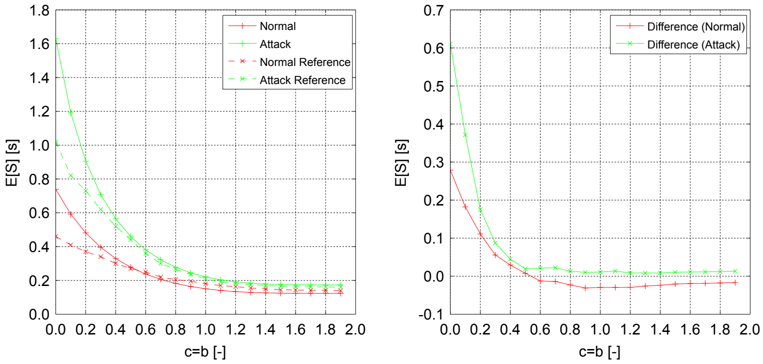


Figure 4-4: Comparison of Sojourn Times Between the Reference and Simulated Results

Further simulations confirmed that the influence of the b parameter is minimal and can be completely omitted in the new protocol approach. The formula (4.4) was accordingly modified, thus only the c parameter was normalised. The difference is in a range of milliseconds, which is negligible, compared to the authentication process in a range of seconds (see Fig. 4-5).

Despite the original DREAM is designed to utilise both parameters, the results presented in Tab. 4-1 and Fig. 4-5 showed that in 400-nodes networks the b parameter influence is negligible regardless of the topology. The same results were obtained when large networks, where the total number of nodes in the network $N \to 10^4$, were examined (see Tab. 4-2).

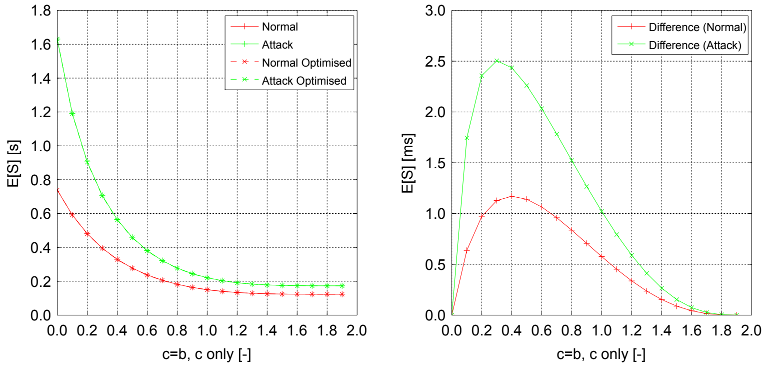


Figure 4-5: Comparison of Sojourn Times Between the Standard and Optimised Simulated Results

The decrease is caused by the fact that the b parameter is only utilised in neighbours of the original transmitter. Because N is significantly greater than $\mathbb{E}[NBR]$, $\mathbb{E}[Deg]$ respectively. Analogous simulations, accomplished for networks where $N < 100$, demonstrated that the $\mathbb{E}[BC_{\text{ratio}}] > 0.05$.

10^6 iterations	Grid	ER	BA	N-ary
$\mathbb{E}[BC_{\text{ratio}}]$ [-]	0.041e-02	0.076e-02	0.019e-02	0.020e-02
$\mathbb{D}[BC_{\text{ratio}}]$ [-]	3.065e-09	2.283e-08	4.634e-08	2.010e-08

Table 4-2: Comparison of BC_{ratio} in Large Networks

However, the application of femtocells is considered to contain hundreds or thousands of access points (as the analogy of the base transceiver stations (BTS) known from the GSM networks). Therefore, the new scheme, named IDARED (which is derived from DREAM), is designed to utilise the c parameter only.

It will be demostrated further that the sojourn time of messages delayed by the authentication mechanism can be improved by the utilisation of a two-queue fork-join system, when examined from the end-to-end delay perspective. The DREAM defends a network node from DoS attacks as per the following mechanism. In the secure mode, all of the incoming messages are sent to the verification queue where been verified. However, assuming the normal mode, based on the probability (equations (1.1) and (1.2)), a node decides whether to send the message to the verification queue or forward the message to its neighbouring nodes directly (to randomly decrease the end-to-end delay).

Either way, the message is sent to the verification queue since it needs to be authenticated. As this queue is manipulated as per first in, first out (FIFO) queuing way, the verification queue does not recognise, which messages were forwarded before being sent to the verification queue or which were sent directly to the verification queue. The red-labelled messages (ID2 a ID3) were forwarded prior being sent to the verification queue. The yellow-labelled message (ID1) was determined to be authenticated first (see Fig. 4-6). The split verification queue design (see Fig. 4-7) has considered the creation of a new low-priority queue. Such queue is dedicated to the verification of all messages which were sent without prior authentication.

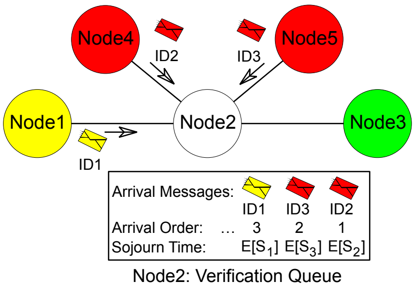


Figure 4-6: Current Mechanism of the Verification Queue

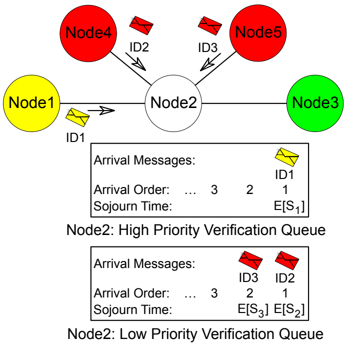


Figure 4-7: Split Verification Queue Mechanism

Considering the split mechanism, the former authentication queue was transformed to a high priority verification queue, as it is determined to authenticate all messages which are marked as "to be authenticated" prior forwarding and the new proposed scheme (outlined in Fig. 4-8) is now influenced by the c parameter only.

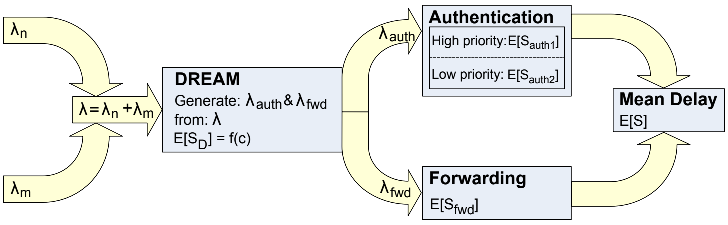


Figure 4-8: Design of the New Proposed Mechanism

Using the same proposed model updated as per Fig. 4-8 and assuming the $c > 0.4$ (see the proposed model limits Fig. 4-4 for details), the split verification queue approach provides significant improvement in the range of tens of percent.

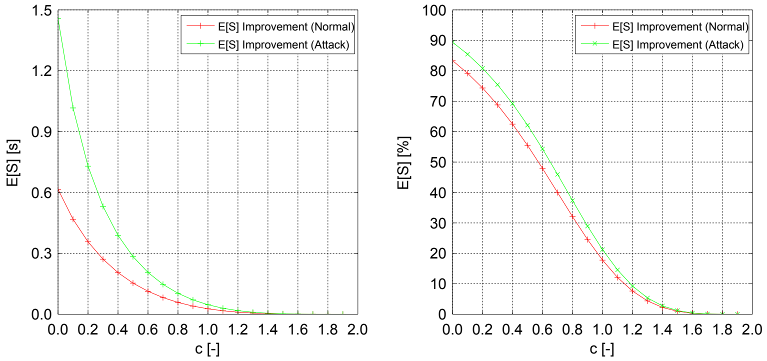


Figure 4-9: Results of the IDARED Compared to DREAM

Along with the increasing probability a message will be forwarded P_{fwd} (the increasing c parameter), the effectiveness of the proposed solution decreases. This is caused by the fact that λ_{auth1} (the flow of messages targeting the high priority authentication queue) rapidly decreases. As the probability a message will be forwarded and authenticated is equal for $c = 0.9$ (assuming the Scenario 1 topology), the $\mathbb{E}[S]$ effectiveness is approximately $25 - 30\%$ (based on λ). Compared to the

DREAM results, the effectiveness of the proposed solution increases if the total flow of messages λ increases (see Fig. 4-9).

The IDARED is a new authentication mechanism to deal with denial-of-service type of attack in broadcast networks. Compared to the DREAM, which it is derived from, it also addresses the stochastic based decision of forwarding messages without prior authentication but it is designed with special emphasis on minimising the average end-to-end delay. Hand in hand with reduction of the internal processes, the energy consumption efficiency increases.

Algorithm 4.1 : Verification and Forwarding Algorithm of IDARED

```
input: An overheard broadcast message $m$
if (overheard messages with the same ($m.ID_{src}$, $m.seqno$) before)
  then return;
end if
if ($m.ID_{fwder}$ is unknown neighbour)
  then return;
end if
$prob = \frac{2 \cdot c}{\|Nbr(m.ID_{fwder})\|}$;
if ($Rand > prob$) then
  // authenticate $m$ first;
  place $m$ into high priority verification queue;
else
  // forward $m$ first;
  rebroadcast $m$;
  place $m$ into low priority verification queue;
end if
```

The internal mechanism of the IDARED is described in Algorithm 4.1. It is apparent that by utilising the c parameter only, the internal processes are reduced compared to the DREAM. From the power point of view, fewer computations cut down the power dissipation [34] and these requirements were addressed by the IDARED. In order to compare the specific internal procedures, a model of the IDARED is described in Fig. 4-10.

Compared to the DREAM, the difference is mainly in application of the split verification queue concept, where the original verification queue is divided into two queues of different priorities. Those messages which were forwarded without prior verification are sent to a low priority queue and the rest of the messages reaches a high priority queue. From the end-to-end perspective, the average delay for messages is decreased since those messages, which were already forwarded without verification, do not bring an extra delay to the messages in the high priority verification queue. The sojourn time increases for messages in low priority queue. However, this introduces an acceptable drawback of the proposed design since either way, all messages are verified before these are processed by the given network device, only in a different order than these arrived.

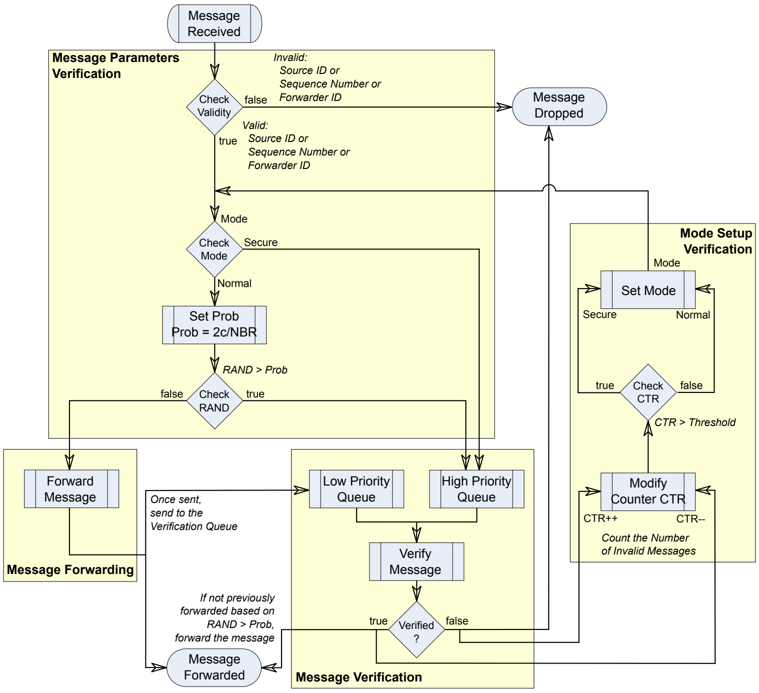


Figure 4-10: Model of the IDARED Mechanism

5 Conclusion

The presented study in this dissertation thesis focused on the design of a new low latency denial of service resistant mechanism for message authentication in a broadcast network. As several papers related to broadcast authentication were already published in the security area of wireless sensor networks, the results and methods were utilised in the future mobile networks approach as well.

The new IDARED is derived from the DREAM scheme which means, the mechanism decides, based on a stochastic condition, whether to authenticate a message prior forwarding or whether to forward it without prior verification. The main advantage of the IDARED over the DREAM, is in application of the split verification queue concept. This approach enables to decrease the mean sojourn time a message spends in the network device and thus, decrease the overall end-to-end delay. The results of the accomplished simulations confirmed, that the mean sojourn time decreased by approximately $25 - 30\%$ for the IDARED, based on the input message flow and assuming the equal probability a message will be authenticated or forwarded without prior verification.

Another benefit of the IDARED is the lower number of used parameters and the smaller protocol data unit. Although, the exact power consumption of the proposed solution is strictly dependent on the utilized hardware of the femtocell device, it was deduced that the power consumption of the IDARED will be lower than for the DREAM. From the above mentioned results it is clear that the designed IDARED scheme can be utilised as a DoS resistant mechanism and can help the mission-critical data delivery in case the network or a part of the network becomes a target of a denial of service attack in the future mobile networks (denoted as the next generation femtocell or the femtocell cloud).

References

[1] HANSMAN, S., HUNT, R. A Taxonomy of Network And Computer Attacks. *Computers & Security*, 2005, vol. 24, no. 1, pp. 31–43. ISSN 0167-4048. doi:10.1016/j.cose.2004.06.011.

[2] HARRISON, K., WHITE, G. A Taxonomy of Cyber Events Affecting Communities. In *44th Hawaii International Conference on System Sciences*, HICSS. 2011, pp. 1–9. ISSN 1530-1605. doi:10.1109/HICSS.2011.37.

[3] PERRIG, A., TYGAR, J. *Secure Broadcast Communication: in Wired and Wireless Networks*. 2nd ed. Norwell, MA, USA: Kluwer Academic Publishers, 2004. 240 p. ISBN 978-0-7923-7650-7.

[4] WOOD, A., STANKOVIC, J. Denial of Service in Sensor Networks. *IEEE Computer*, 2002, vol. 35, no. 10, pp. 54–62. ISSN 0018-9162. doi:10.1109/MC.2002.1039518.

[5] GAN, X., LI, Q. A Multi-user DoS-Containment Broadcast Authentication Scheme for Wireless Sensor Networks. In *Proceedings of the International Conference on Information Technology and Computer Science, ITCS 2009*, vol. 1. 2009, pp. 472–475. ISBN 978-0-7695-3688-0-01. doi:10.1109/ITCS.2009.103.

[6] PERRIG, A., SONG, D., CANETTI, R., ET AL. *Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction*, [Online]. Carnegie Mellon University, IBM, University of California, Berkeley, BT, USA, 2005 [cit. 2012–06–19]. Available from WWW: <`http://tools.ietf.org/html/rfc4082`>.

[7] VANĚK, T. *Formální modely všesměrových autentizačních protokolů*. Dissertation Thesis. Czech Republic: Czech Technical University in Prague, Faculty of Electrical Engineering, Department of Telecommunication Engineering, 2008. 85 p.

[8] VANĚK, T., ROHLÍK, M. Simulation of the Selected Network Attacks on the TESLA Authentication Protocol. In *Proceedings of the 6th International Conference on Digital Technologies [CD-ROM], DT2009*, vol. 1. Žilina, Slovak Republic: University of Zilina, 2009, pp. 1–2. ISBN 978-80-554-0150-8.

[9] HUANG, Y., HE, W., NAHRSTEDT, K., ET AL. DoS-Resistant Broadcast Authentication Protocol with Low End-to-end Delay. In *IEEE INFOCOM Workshops 2008*. Phoenix, AZ, USA, 2008, pp. 1–6. ISBN 978-1-4244-2219-7. doi:10.1109/INFOCOM.2008.4544589.

[10] VANĚK, T., ROHLÍK, M. Model of DoS Resistant Broadcast Authentication Protocol in Colored Petri Net Environment. In *Proceedings of the 17th International Conference on Systems, Signals and Image Processing*, IWSSIP 2010. Rio de Janeiro, Brazil, 2010, pp. 264–267. ISBN 978-85-228-0565-5. doi:10.1145/1288107.1288118.

[11] ASLAM, N., ROBERTSON, W., PHILLIPS, W. Performance Analysis of WSN Clustering Algorithms Using Discrete Power Control. *IPSI Transactions on Internet Research*, 2009, vol. 5, no. 1, pp. 10–15. ISSN 1820-4503.

[12] ACHIR, M., OUVRY, L. Power Consumption Prediction in Wireless Sensor Networks. In *Proceedings of the 16th ITC Specialist Seminar on Performance Evaluation of Wireless and Mobile Systems*. 2004. doi:10.1.1.60.1065.

[13] CHEE, D., SUK KANG, M., LEE, H., ET AL. A Study on the Green Cellular Network with Femtocells. In *Third International Conference on Ubiquitous and Future Networks*, ICUFN 2011. 2011, pp. 235–240. ISBN 978-1-4577-1176-3. doi:10.1109/ICUFN.2011.5949168.

[14] DI ZENOBIO, D., CELIDONIO, M., PULCINI, L., ET AL. An Integrated Access Network Infrastructure Combining Femtocells to Existing Cabled Networks. In *Wireless Telecommunications Symposium*, WTS 2011. 2011, pp. 1–5. ISSN 1934-5070. doi:10.1109/WTS.2011.5960880.

[15] O'CARROLL, J., CLAUSSEN, H., DOYLE, L. Partial GSM Spectrum Reuse for Femtocells. In *20th International Symposium on Personal, Indoor and Mobile Radio Communications*, IEEE. 2009, pp. 2111–2116. ISBN 978-1-4244-5123-4. doi:10.1109/PIMRC.2009.5449865.

[16] KNISELY, D. N., YOSHIZAWA, T., FAVICHIA, F. Standardization of Femtocells in 3GPP. *IEEE Communications Magazine*, 2009, vol. 47, no. 9, pp. 68–75. ISSN 0163-6804. doi:10.1109/MCOM.2009.5277458.

[17] KNISELY, D. N., FAVICHIA, F. Standardization of Femtocells in 3GPP2. *IEEE Communications Magazine*, 2009, vol. 47, no. 9, pp. 76–82. ISSN 0163-6804. doi:10.1109/MCOM.2009.5277459.

[18] I.SALAMA, G., SHEHAB, M. E., HAFEZ, A. A., ET AL. Performance Analysis of Transmitting Voice over Communication Links Implementing IPsec. In *13th International Conference on Aerospace Sciences and Aviation Technology*, [Online]. 2009, pp. 1–12. ISSN 2090-0678. Available from WWW: <`http://www.mtc.edu.eg/ASAT13/pdf/CE13.pdf`>.

[19] FREEDOM *Femtocell-based Network Enhancement by Interference Management and Coordination of Information for Seamless Connectivity*. Specific Targeted Research Project (STREP) of the 7th Framework Programme, 2011 [cit. 2012–06–19]. Available from WWW: <`http://www.ict-freedom.eu`>.

[20] PÜSCHEL, J. *Why Should Operators Deploy Wi-Fi and Femtocell?* 2011 [cit. 2012–06–19]. Available from WWW: <`http://blogs.informatandm.com/why-should-operators-deploy-wi-fi-and-femtocell`>.

[21] GOS NETWORKS. *The #Cloud Will Force the #Femtocell to Evolve*. 2011 [cit. 2012–06–19]. Available from WWW: <`http://blog.gosnetworks.com/blog/the-cloud-will-force-the-femtocell-to-evolve`>.

[22] TSAO, K.-J., SHEN, S.-C., HOU, T.-C. Location-Dependent Power Setting for Next Generation Femtocell Base Stations. In *IEEE Wireless Communications and Networking Conference*, WCNC. 2011, pp. 767–772. ISBN 978-1-61284-255-4. ISSN 1525-3511. doi:10.1109/WCNC.2011.5779229.

[23] VANĚK, T., ROHLÍK, M. Alternative Protocols for Femtocell Backbone Security. In *4th Joint IFIP Wireless and Mobile Networking Conference*. Piscataway, NJ, USA: IEEE Press, 2011, pp. 1–4. ISBN 978-1-4577-1191-6. doi:10.1109/WMNC.2011.6097239.

[24] ZOU, X., RAMAMURTHY, B., MAGLIVERAS, S. S. *Secure Group Communications Over Data Networks*. 1st ed. USA: Springer Science+Business Media, Inc., 2005. 172 p. ISBN 978-0-387-22970-6.

[25] ROHLÍK, M., VANĚK, T. Broadcast Authentication Mechanism Optimization. In *13th International Conference on Research in Telecommunication Technologies – Vol. II Poster Section [CD-ROM]*, RTT2011. Brno, Czech Republic: Brno University of Technology, Faculty of Electrical Engineering and Communication, 2011, pp. 40–43. ISBN 978-80-214-4283-2.

[26] VANĚK, T., ROHLÍK, M. Optimization of DoS Resistant Broadcast Authentication Mechanism. In *Proceedings of the Networking and Electronic Commerce Research Conference*, NAEC2011. Dallas, TX, USA: American Telecommunications Systems Management Association Inc., 2011, pp. 139–143. ISBN 978-0-9820958-5-0.

[27] BLINDER, P. *Erdos-Renyi Random Graph*. 2005 [cit. 2012–06–19]. Available from WWW: <`http://www.mathworks.com/matlabcentral/fileexchange/4206-erdos-renyi-random-graph`>.

[28] GEORGE, M. *B-A Scale-Free Network Generation and Visualization*. 2007 [cit. 2012–06–19]. Available from WWW: <`http://www.mathworks.com/matlabcentral/fileexchange/11947`>.

[29] Gowers, T., Barrow-Green, J., Leader, I. (ed.) *The Princeton Companion to Mathematics*. Princeton University Press, 2008. 1008 p. ISBN 978-0-6911-1880-2.

[30] WU, J., TAN, Y.-J., DENG, H.-Z., ET AL. A New Measure of Heterogeneity of Complex Networks Based On Degree Sequence. In *Unifying Themes in Complex Systems*. Springer-Verlag Berlin Heidelberg, 2010, pp. 66–73. ISBN 978-3-540-85081-6. doi:10.1007/978-3-540-85081-6_9.

[31] VIJAYAKUMAR, P., BOSE, S., KANNAN, A., ET AL. An Effective Key Distribution Protocol for Secure Multicast Communication. In *Second International Conference on Advanced Computing*, ICoAC. 2010, pp. 102–107. ISBN 978-1-61284-261-5. doi:10.1109/ICOAC.2010.5725367.

[32] ADAN, I., RESING, J. *Queueing Theory*, [Online]. 2002 [cit. 2012–06–19], 180 pp. Available from WWW: <`http://www.win.tue.nl/~iadan/queueing.pdf`>.

[33] KEMPER, B., MANDJES, M. Mean Sojourn Times in Two-Queue. Fork-Join Systems: Bounds and Approximations. In *OR Spectrum*, vol. 291. Springer-Verlag Berlin Heidelberg, 2011, pp. 1–20. ISBN 978-3-540-85081-6. doi:10.1007/s00291-010-0235-y.

[34] WADLEIGH, K. R., CRAWFORD, I. L. *Software Optimization for High Performance Computing: Creating Faster Applications*. 1st ed. Prentice Hall, 2000. 377 p. ISBN 978-0-130-17008-8.

List of Candidate's Work Related to the Thesis

Impact

[1] VANĚK, T., ROHLÍK, M. Analysis of Broadcast Authentication Mechanism in Selected Network Topologies. *Radioengineering*, 2010, vol. 20, no. 1, pp. 167–173. ISSN 1210-2512. doi:10.2298/CSIS110227057Q, (50 %).

Reviewed

None.

Patents

None.

Web of Science

See "Impact" section above.

Others

[1] VANĚK, T., ROHLÍK, M. Simulation of the Selected Networks Attack to the TESLA Authentication Protocol. In *Proceedings of the 6th International Conference on Digital Technologies [CD-ROM]*, DT2009. Žilina, Slovak Republic: TU v Žilině, 2009, pp. 1–2. ISBN 978-80-554-0150-8. (50 %).

[2] ROHLÍK, M., VANĚK, T. Broadcast Authentication Mechanism Optimization in Fully N-ary Tree Topology. In *Proceedings of the Knowledge in Telecommunication Technologies and Optics [CD-ROM]*, KTTO 2010. Ostrava, Czech Republic: VŠB – TUO, FEI, Katedra elektroniky a telekomunikační techniky, 2010, pp. 111–114. ISBN 978-80-248-2330-0. (50 %).

[3] ROHLÍK, M., VANĚK, T. Effectivity Optimization of Femtocell Backbone Security Methods. In *Proceedings of the 12th International Conference on Research in Telecommunication and Technology [CD-ROM]*, RTT 2010. Ostrava, Czech Republic: VŠB – TUO, FEI, Katedra elektroniky a telekomunikační techniky, 2010, pp. 142–146. ISBN 978-80-248-2261-7. (50 %).

[4] ROHLÍK, M., VANĚK, T. Optimization of Femtocell IP Backbone Security Mechanisms. In *Proceedings of the Networking and Electronic Commerce Research Conference*, NAEC 2010. Dallas, TX, USA: American Telecommunications Systems Management Association Inc., 2010, pp. 167–176. ISBN 978-0-9820958-3-6. (50 %).

[5] VANĚK, T., ROHLÍK, M. Model of DoS Resistant Broadcast Authentication Protocol in Coloured Petri Net Environment. In *Proceedings of the 17th International Conference on Systems, Signals and Image Processing [CD-ROM]*, IWSSIP 2010. Rio de Janeiro, Brazil: EdUFF – Editora da Universidade Federal Fluminense, 2010, pp. 264–267. ISBN 978-85-228-0565-5. doi:10.1145/1288107.1288118, (50 %).

[6] ROHLÍK, M., VANĚK, T. Broadcast Authentication Mechanism Optimization. In *Proceedings of the 13th International Conference on Research in Telecommunication Technologies 2011 – Vol. II Poster Section [CD-ROM]*, RTT 2011. Brno, Czech Republic: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011, pp. 40–43. ISBN 978-80-214-4283-2. (50 %).

[7] ROHLÍK, M., VANĚK, T. Femtocell Backhaul Security Efficiency. In *Proceedings of the 11th International Conference Knowledge in Telecommunication Technologies and Optics [CD-ROM]*, KTTO 2011. Ostrava, Czech Republic: VŠB – TUO, FEI, Katedra elektroniky a telekomunikační techniky, 2011, pp. 145–148. ISBN 978-80-248-2399-7. (50 %).

[8] VANĚK, T., ROHLÍK, M. Alternative Protocols for Femtocell Backbone Security. In *4th Joint IFIP Wireless and Mobile Networking Conference*. Piscataway, NJ, USA: IEEE Press, 2011, pp. 1–4. ISBN 978-1-4577-1191-6. doi:10.1109/WMNC.2011.6097239, (50 %).

[9] VANĚK, T., ROHLÍK, M. Optimization of DoS Resistant Broadcast Authentication Mechanism. In *Proceedings of the Networking and Electronic Commerce Research Conference*, NAEC2011. Dallas, TX, USA: American Telecommunications Systems Management Association Inc., 2011, pp. 139–143. ISBN 978-0-9820958-5-0. (50 %).

Projects

[1] ROHLÍK, M. (co-researcher). Aspekty mobility v moderních bezdrátových sítích. ČVUT v Praze, Fakulta elektrotechnická, 2010, Grant SGS, No. SGS10/274/OHK3/3T/13.

[2] ROHLÍK, M. (co-researcher). Femtocell-based Network Enhancement by Interference Management and Coordination of Information for Seamless Connectivity. Specific Targeted Research Project (STREP) of the 7th Framework Programme of the European Commission, 2010, Grant FREEDOM. Available from WWW: <http://www.ict-freedom.eu>.

List of Candidate's Work Non-Related to the Thesis

Impact

None.

Reviewed

[1] ROHLÍK, M. Vytváření podsítí s proměnnou maskou v prostředí IPv4 [Online]. *Access Server*, 2009, vol. 7, no. 200903, p. 0001. ISSN 1214-9675. Available from WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2009030001>. (100 %).

[2] ROHLÍK, M. Využití proudových šifer v současnosti [Online]. *Access Server*, 2009, vol. 7, no. 200908, p. 0001. ISSN 1214-9675. Available from WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2009080001>. (100 %).

[3] ROHLÍK, M. Co umí zařízení Signamax. *Connect!*, 2010, vol. XV, no. 3/2010, pp. 32–33. ISSN 1211-3085. (100 %).

[4] ROHLÍK, M., LAFATA, P. Bezpečnostní rizika v současné generaci pasivních optických přístupových sítí [Online]. *Elektrorevue*, 2010, vol. 13, no. 37, pp. 1–6. ISSN 1213-1539. Available from WWW: <http://elektrorevue.cz/cz/download/bezpecnostni-rizika-v-soucasne-generaci-pasivnich-optickych-pristupovych-siti>. (50 %).

[5] ROHLÍK, M., LAFATA, P. Bezpečnostní rizika v současné generaci PON. *Sdělovací technika*, 2010, vol. 58, no. 10/2010, pp. 5–8. ISSN 0036-9942. (50 %).

[6] LAFATA, P., ROHLÍK, M. Konfigurace a testování triple play služeb v pasivní optické síti [Online]. *Elektrorevue*, 2011, vol. 14, no. 3, pp. 1–9. ISSN 1213-1539. Available from WWW: <http://elektrorevue.cz/cz/download/konfigurace-a-testovani-triple-play-sluzeb-v-pasivni-opticke-siti>. (50 %).

[7] CHMELA, L., ROHLÍK, M., KOPP, M. *Průvodce oborovou didaktikou pro učitele telekomunikačních předmětů na technické vysoké škole*. vol. 1. Praha, Czech Republic: České vysoké učení technické v Praze, 2011. 82 p. ISBN 978-80-01-04794-1, (5 %; 90 - 5 - 5 %).

Patents

[1] ROHLÍK, M. Univerzální nástroj pro návrh sítě v prostředí IPv4 (Autorizovaný SW) [Online]. ČVUT v Praze, Fakulta elektrotechnická, Katedra telekomunikační techniky, 2009, Available from WWW: `http://matlab.feld.cvut.cz/view.php?cisloclanku=2009020002`.

Web of Science

None.

Others

[1] ROHLÍK, M. Professional Interactive Voice Response System. In *Proceedings of the 11th International Conference on Research in Telecommunication and Technology [CD-ROM]*, RTT 2008. Bratislava, Slovak Republic: STU v Bratislavě, 2008, pp. 1–3. ISBN 978-80-227-2939-0. (100 %).

[2] ROHLÍK, M. Innovation of Laboratory Courses in the subject Communication in Data Networks. In *Proceedings of the 12th International Workshop on Research in Telecommunication and Technology [CD-ROM]*, wRTT2009. Praha, Czech Republic: České vysoké učení technické v Praze, 2009, p. 0053_0018. ISBN 978-80-01-04411-7. (100 %).

[3] ROHLÍK, M. Inovace laboratorních kurzů v předmětu Informační bezpečnost a utajování datových zpráv. In *Proceedings of the 13th International Workshop on Research in Telecommunication and Technology [CD-ROM]*, wRTT2010. Ostrava, Czech Republic: VŠB – TUO, FEI, Katedra elektroniky a telekomunikační techniky, 2010, pp. 59–61. ISBN 978-80-248-2262-4. (100 %).

Projects

[1] ROHLÍK, M. (researcher). Inovace laboratorních cvičení předmětu Komunikace v datových sítích. ČVUT v Praze, Fakulta elektrotechnická, 2009, Grant FRVŠ, No. 178/2009/G1.

[2] ROHLÍK, M. (co-researcher). Implementace moderních výukových metod do telekomunikačních studijních předmětů. ČVUT v Praze, Fakulta elektrotechnická, 2009, Grant FRVŠ, No. 211/2009/G1.

[3] ROHLÍK, M. (researcher). Inovace laboratorních cvičení předmětu Informační bezpečnost a utajování zpráv. ČVUT v Praze, Fakulta elektrotechnická, 2010, Grant FRVŠ, No. 605/2010/G1.

Summary

A typical broadcast authentication communication within information distribution systems is characterised by plain text communication between nodes, which do not mutually authenticate. To provide the respective access control key distribution, transmissions sources authentication, and streams non-repudiation, specific authentication protocols were designed. Although, the authentication of every incoming message seems to be a very effective way to mitigate a denial of service type attack, such process results into an increase of end-to-end delay. To mitigate this drawback, the broadcast authentication protocols have been proposed.

This dissertation thesis introduces a new IDARED mechanism, which is based on a DREAM authentication scheme. IDARED provides lower latency results for end-to-end data traffic, which was achieved by several parameters optimisation and a split verification queue concept. The results are examined theoretically and using simulations in MATLAB® environment as well.

Keywords: authentication, broadcast security, DoS, DREAM, IDARED, latency, mechanism, next generation femtocell, protocol

Anotace

Typická autentizace všesměrové komunikace v distribuovaných informačních systémech se vyznačuje komunikací v otevřené formě mezi jednotlivými uzly, které se navzájem neautentizují. Aby byla zajištěna odpovídající distribuce přístupových klíčů, vzájemná autentizace vysílačů a doručení datových zpráv, byly navrženy specifické autentizační protokoly. Ačkoliv se autentizace každé, do uzlu přicházející, zprávy jeví jako účinné řešení pro potlačení útoků typu zamezení/odmítnutí služby (denial of service), takovýto způsob zvyšuje celkové zpoždění přenosu zprávy mezi koncovými prvky sítě (end-to-end delay). Pro potlačení této nevýhody byly navrženy všesměrové autentizační protokoly.

Tato dizertační práce představuje nový mechanismus IDARED založený na autentizačním schématu DREAM. IDARED umožňuje nižší zpoždění pro datový přenos mezi koncovými uzly sítě pomocí optimalizace některých parametrů a konceptu rozdělené ověřující fronty. Výsledky jsou ověřeny teoreticky a rovněž v prostředí MATLAB® pomocí příslušných simulací.

Klíčová slova: autentizace, DoS, DREAM, femtobuňky nové generace, IDARED, mechanismus, protokol, všesměrová bezpečnost, zpoždění