Broadcast Security in Future Mobile Networks

M. Rohlik[1], T. Vanek[1]
[1]*Department of Telecommunication Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Technicka 2, 166 27 Prague 6, Czech Republic*
matej.rohlik@fel.cvut.cz

***Abstract*—A typical broadcast authentication communication within information distribution systems is characterised by plain text communication between nodes, which do not mutually authenticate. 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 paper introduces a new improved delay and resource enhanced DREAM (IDARED) scheme, which is based on the DoS resistant efficient authentication mechanism (DREAM) and which provides lower latency results achieved by several parameters optimisation and a split verification queue concept for the end-to-end management data traffic in the next generation femtocell (NGF).**

***Index Terms*—Authentication, femtocloud, femtocell, security.**

I. INTRODUCTION

The demand for mobile high data rate traffic has been increasing as a consequence of a large nomadic population and the type of applications to be utilised. Therefore, the efficiency of the evolving 5G networks needs to be enhanced in terms of spectrum, energy, cost and security. These demands can be solved by leveraging femtocells, which are considered by several mobile operators and different standards such as mobile WiMAX (IEEE 802.16m) and LTE-Advanced [1], [2].

Network technologies develop very fast as well as data services provided via mobile data networks. As a result, the total available end user bandwidth increases and the end-to-end delay decreases enabling the delay sensitive services (such as broadcast audio/video streams) to be provided to the customers via mobile networks. The emerging cloud computing technology enables new services (e.g. computing resources, storage) to be delivered. However, besides such services, complex challenges emerge. These are related to confidentiality, integrity and availability of the transmitted data and applications. Such mission-critical broadcast data streams require confidentiality and need to be protected from eavesdropping, replay attacks, malicious denial of service (DoS) attacks and other threats.

Although not fully standardised yet, secure group protocols were proposed to resolve the previously mentioned challenges [3], [4]. In addition, a DoS resistant efficient authentication mechanism (DREAM) [5] was designed to deal with DoS types of attacks with the emphasis on the end-to-end delay.

As the mechanisms were defined generally, the specific application in femtocell cloud (femtocloud) environment will be further analysed within the scope of this paper, which introduces a new authentication improved delay and resource enhanced DREAM (IDARED) scheme that is based on the DREAM. The IDARED provides lower latency results for end-to-end data traffic, mainly achieved by split verification queue concept and optimisation of several parameters to improve user experience on latency and download/upload speed, thus covering requirements defined by the TROPIC project [6].

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 [7]. 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 [8].

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, authentication of data sources, 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 [4].

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

Manuscript received March 19, 2014; accepted September 19, 2014.

cope with malicious network threats as the denial of service (DoS) type attacks. In [9], 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.

II. SECURITY OF BROADCAST COMMUNICATION

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 as well. 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 [10].

In a 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). However, 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 (source transmitter MAC key is known). Therefore, an asymmetric algorithm based on digital signatures is necessary for such purpose [11].

In broadcast networks, it is essential to authenticate a single transmitter to more than one receiver. 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 increases the total delay from the end-to-end perspective. None of the currently applied broadcast security protocols does effectively deal with DoS type attacks and does minimise the end-to-end delay to prevent the overall energy depletion [12]. Therefore, this research work provides enhanced framework based on DoS resistant efficient authentication mechanism (DREAM) [5] approach.

A. Design of DREAM

Besides DoS, the DREAM mitigates the DDoS impact by involving more stations in the verification process (see Figure 1). 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 [13]:

– *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.

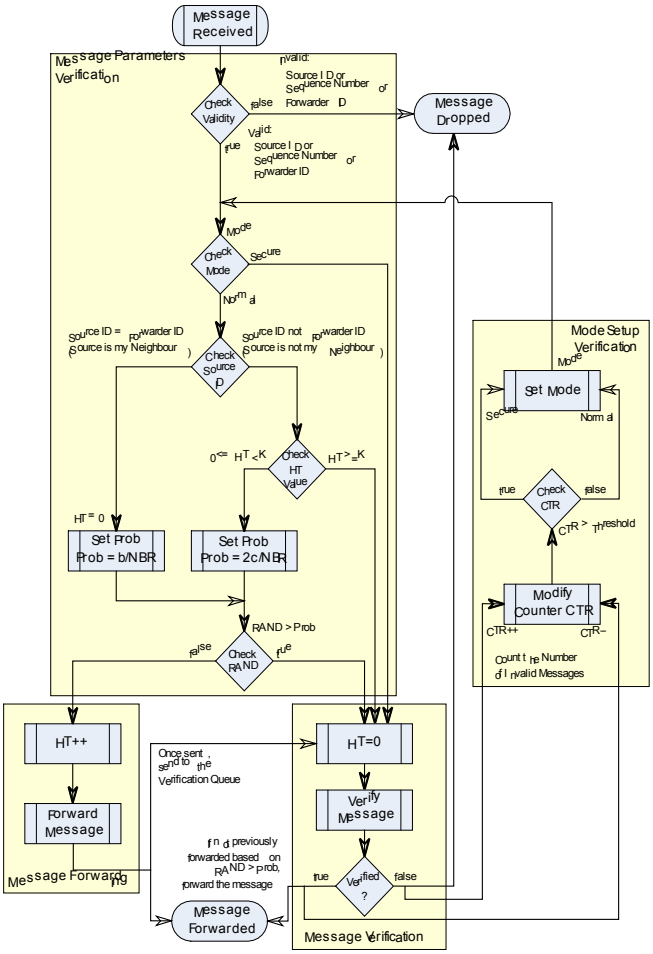


Fig. 1. Model of the DREAM protocol.

The node decides to authenticate/forward the message according to the result of (1), 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 (2), in case the message did not come from a direct neighbour, the neighbour has not been verified, or the parameter $HT > 0$:

$$\text{Rand} > \frac{b}{NBR}, \tag{1}$$

$$\text{Rand} > \frac{2 \times c}{NBR}, \tag{2}$$

where *Rand* is a random number generated by every node for every message in the range of 0 and 1 with the uniform distribution.

This approach enables to save energy resources of the network devices especially when they are under attack [5]. The emphasis on minimal energy consumption is common as well as the security and DoS resistance for both the sensor networks and femtocells designs [14]–[16].

B. Femtocells

The femtocell is a very low-power 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 home evolved NodeBs (HeNBs) are designed for use without any supervision of the macrocell [17].

The security aspects of HeNB communication were part of the FREEDOM project [18]. 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. Such deployment introduces a network cloud in the femtocell environment. To distinguish the current femtocell from the previously described approach, it is designated as the next generation femtocell (NGF) in this paper. The authors in [19] use the NGF term in a more general way as they consider it as the future technology but they do not discuss any specific options nor the cloud feature at all.

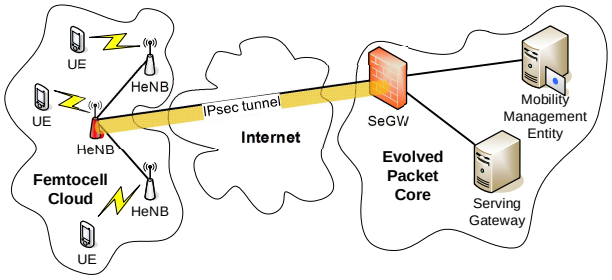


Fig. 2. The next generation femtocell deployment (Femtocell Cloud).

The HeNBs are commonly connected to the mobile operator network via secured tunnels to the security gateway (SeGW). However, in the NGF deployment the HeNBs are interconnected and enabled to communicate among them as well – direct HeNB-to-HeNB connectivity (see Fig. 2). The HeNBs do have connectivity to respective resources (data storages, database servers, and other servers) based on the service offered by the mobile operator [20].

From the previous discussion can be seen that the sensor networks and future mobile environments address analogous security, energy consumption, and parameter requirements. Therefore, this paper 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.

III. 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.

A. Mathematical Model of the DREAM

Based on the probability decision ((1) and (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 (3) is apparent

$$P_{auth} = 1 - P_{fwd}. \tag{3}$$

Reference data were obtained from [5] and the arrival and service rates were estimated as exponential. Although, the $\lambda = \lambda_n + \lambda_m$ offered to the network node is known (normal user data arrival rate is denoted as λ_n and the malicious user data arrival rate as λ_m), the DREAM produces two flows of messages: messages to be delivered to the authentication queue λ_{auth} and messages to be forwarded λ_{fwd}. Basically, this process depends on parameters *b*, *c*, and *K*.

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)

$$P_{fwd} = p_1 \times p_2 \times \cdots \times p_{NHR} = p^{NHR}, \tag{4}$$

where $p_1 = p_2 = \cdots = p_{NHR} = p$ 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* parameters (which are the normalized *b* and *c* parameters discussed further, see formulae (6) and (7), 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 per cent (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 ($K = NHR$), the respective limit values of the *K* parameter can be calculated analogically (see results for selected values of *C* in Fig. 3).

For a comparison purpose, the simulations were accomplished 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).

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.

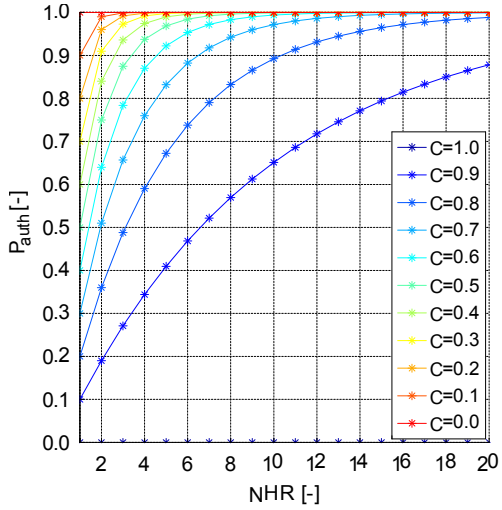


Fig. 3. Message authentication probability.

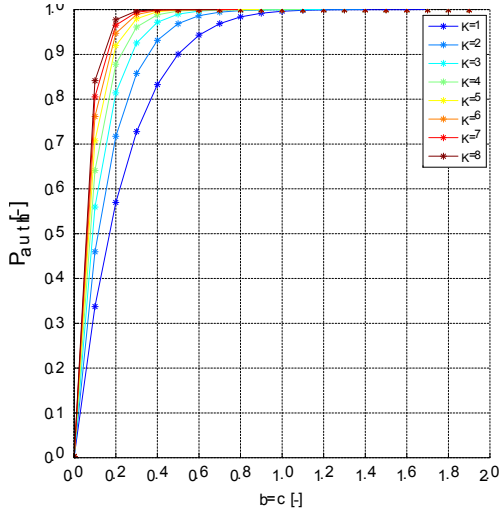


Fig. 4. Influence of the K parameter on message authentication probability.

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 (5)

$$P_{auth} = \frac{p_b \times B + p_c \times C}{p_b + p_c}, \tag{5}$$

where *B* and *C* are normalised *b* and *c* parameters as per (6) and (7). It is apparent, 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*:

$$\mathrm{B} = 1 - \frac{b}{b_{max}} = 1 - \frac{b}{NBR}, \tag{6}$$

$$\mathrm{C} = 1 - \frac{c}{c_{max}} = 1 - \frac{2 \times c}{NBR}. \tag{7}$$

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 [5], the results were highlighted for a special case, where *b* = *c*, for further comparison.

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. The result $P^{\square}_{auth}$ is corresponding to the grid network represented by formula (8) and exponential dependency (Fig. 5).

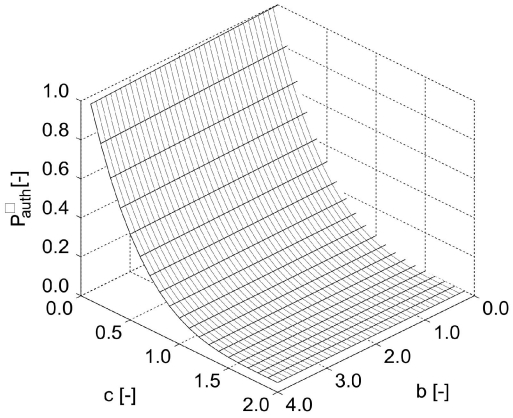


Fig. 5. Influence of parameters on authentication probability.

$$P^{\square}_{auth} = EDS \times (P_{auth})^{NBR}, \tag{8}$$

where *EDS* is the entropy of degree sequence and *NBR* is the mean number of neighbours. The complete $P^{\square}_{auth}$ can be expressed as per (9).

$$P^{\square}_{auth} = EDS \times \left(\frac{p_b \times \left(1 - \frac{b}{NBR}\right) + p_c \times \left(1 - \frac{2 \times c}{NBR}\right)}{p_b + p_c} \right)^{NBR}. \tag{9}$$

B. Operating Conditions of the Model

The proposed model behaviour (the course of $\mathbb{E}(S)$) was studied under normal conditions ($^{a}_{m} = 0$) as well as in case a network device is under attack, thus being flooded by a huge amount of messages ($^{a}_{m} > 0$). Compared with [5], 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. 6).

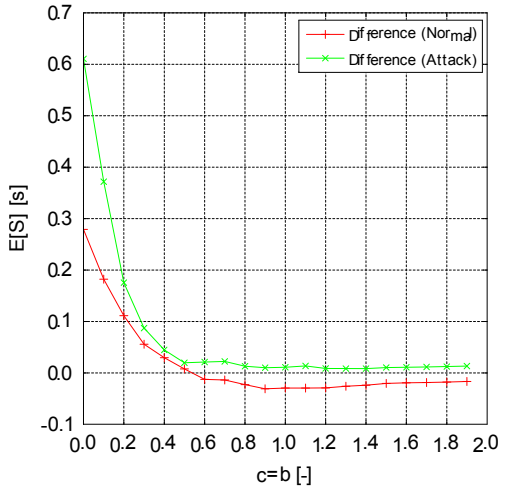
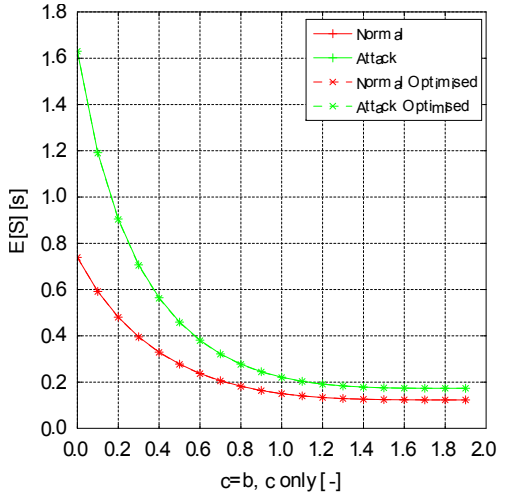
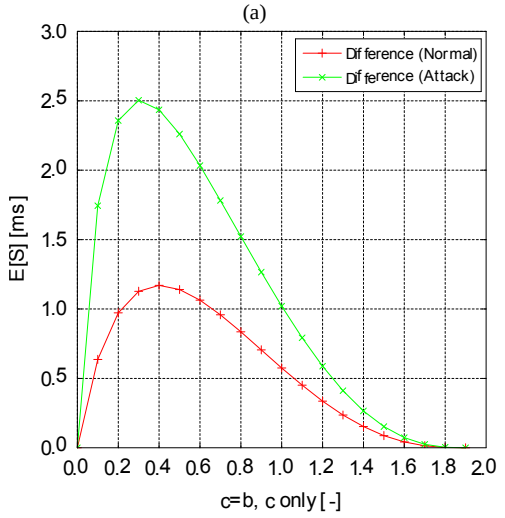


Fig. 6. Comparison of sojourn times between the reference and simulated results.



(a)



(b)

Fig. 7. Comparison of sojourn times between the standard (a) and optimised (b) 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 equation (5) was accordingly modified, thus only the *c* parameter was normalised. The difference is in the range of milliseconds, which is negligible, compared to the authentication process in the range of seconds (see Fig. 7).

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 $\mathbb{E}[NBR]$ and $\mathbb{E}[Deg]$ respectively. Analogous simulations, accomplished for networks where $N < 100$, demonstrated that the $\mathbb{E}\left[BC_{ratio}\right] > 0.05$. 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 demonstrated 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.

IV. Mathematical Model of the IDARED

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 (1) and (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).

A. Design of the Proposed Mechanism

Either way, the message is sent to the verification queue since it needs to be authenticated. Since 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 and ID3) were forwarded prior being sent to the verification queue. The yellow-labelled message (ID1) was determined to be authenticated first (see Fig. 8). The split verification queue design (see Fig. 9) 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.

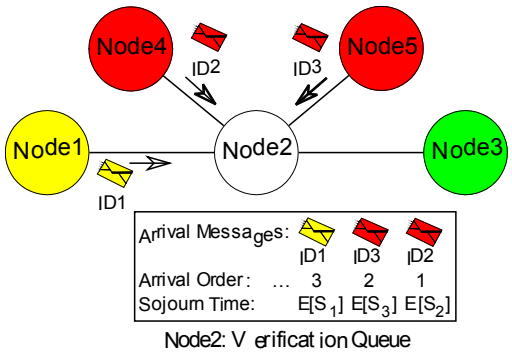


Fig. 8. Current mechanism of the verification queue.

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. 10) is now influenced by the c parameter only.

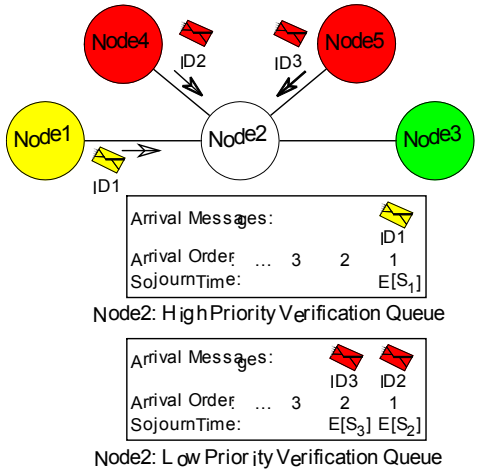


Fig. 9. Split verification queue mechanism.

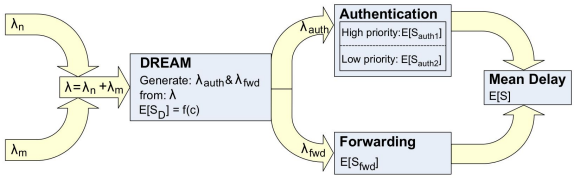


Fig. 10. Design of the new proposed mechanism (IDARED).

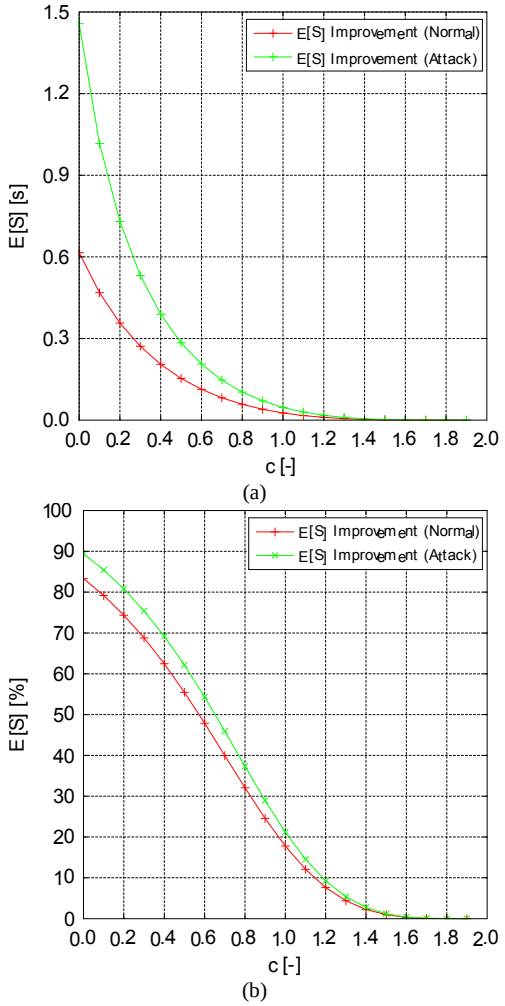


Fig. 11. Results of the IDARED (a) compared to DREAM (b).

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_{auth} (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 $c = 0.9$, 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. 11).

B. *New Scheme Summary*

As addressed by the IDARED, utilising the c parameter only, the internal processes are reduced compared to the DREAM (see Algorithm 1). From the power perspective, fewer computations cut down the power dissipation [21].

Algorithm 1 : Mechanism of the IDARED

input: An overheard broadcast message m

if (duplicate message (same $m.ID_{src}$ or $m.seqno$))
  then return;
end if
if ($m.ID_{fwder}$ is unknown neighbour)
  then return;
end if
$prob = \dfrac{2 \cdot c}{||Nbr(m.ID_{fwder})||}$;
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

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 (see Fig. 12).

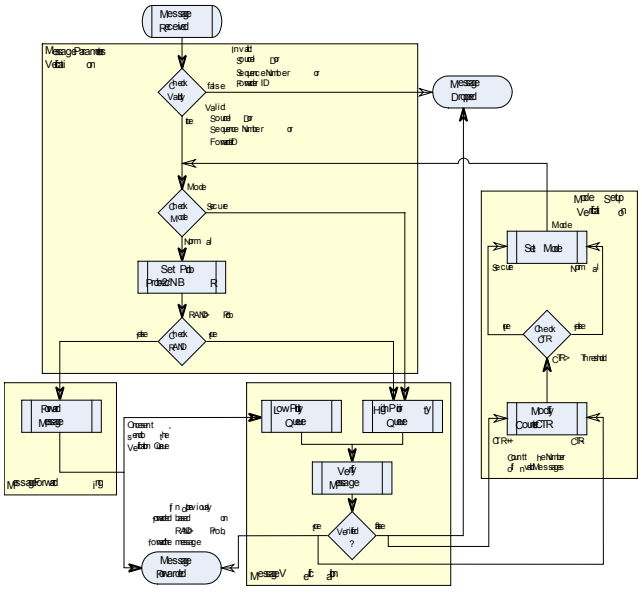


Fig. 12. Model of the IDARED Mechanism.

Those messages which were forwarded without prior verification are sent to a low priority queue and the rest of the messages reach a high priority queue. From the end-to-end perspective, the average delay of 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.

V. CONCLUSIONS

The presented research is focused on the design of a new low latency denial of service resistant mechanism of message authentication in a broadcast network.

The broadcast concept is presented as efficient for management data traffic of cloud computing services in the next generation femtocloud which is supposed to provide appropriate means to support high demanding applications and is considered to be the part of future 5G networks.

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. Therefore, the designed IDARED scheme can be utilised as a DoS resistant mechanism and can help the mission-critical data delivery in cases where any of the network part becomes a target of a DoS attack in the cloud environment of the next generation femtocell networks. Real environment tests and the power efficiency of the proposed approach have not yet been examined and are a challenge for further studies.

REFERENCES

[1] IEEE, Standard for local and metropolitan area networks part 16: Air interface for broadband wireless access systems amendment 3: Advanced air interface (IEEE 802.16m), USA, 2011. [Online] Available: http://standards.ieee.org/getieee802/download/802.16m-2011.pdf

[2] H. Holma, A. Toskala, *LTE for UMTS: Evolution to LTE-Advanced*. United Kingdom: John Wiley & Sons, Ltd., 2011. [Online]. Available: http://dx.doi.org/10.1002/9781119992943

[3] X. Zou, B. Ramamurthy, S. S. Magliveras, *Secure Group Communications Over Data Networks*. USA: Springer Science+Business Media, Inc., 2005.

[4] A. Perrig, J. Tygar, *Secure Broadcast Communication: in Wired and Wireless Networks*. Norwell, MA, USA: Kluwer Academic Publishers, 2004.

[5] Y. Huang, W. He, K. Nahrstedt, W. Lee, "DoS-resistant broadcast authentication protocol with low end-to-end delay", in *IEEE INFOCOM Workshops*, Phoenix, AZ, USA, 2008, pp. 1–6. [Online] Available: https://dx.doi.org/10.1109/INFOCOM.2008.4544589

[6] TROPIC, Distributed computing, storage and radio resource allocation over cooperative femtocells, Specific Targeted Research Project of the 7th Framework Programme (2012). [Online] Available: http://www.ict-tropic.eu

[7] S. Hansman, R. Hunt, "A taxonomy of network and computer attacks", *Computers & Security*, vol. 24, no. 1, pp. 31–43, 2005. [Online] Available: https://dx.doi.org/10.1016/j.cose2004.06.011

[8] K. Harrison, G. White, "A taxonomy of cyber events affecting communities", in *44th Hawaii Int. Conf. System Sciences, (HICSS)*, 2011, pp. 1–9. [Online] Available: https://dx.doi.org/10.1109/HICSS.2011.37

[9] A. Wood, J. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, vol. 35, no. 10, pp. 54–62, 2002. [Online] Available: https://dx.doi.org/10.1109/MC.2002.1039518

[10] X. Gan, Q. Li, "A multi-user DoS-containment broadcast authentication scheme for wireless sensor networks", in *Proc. Int. Conf. Information Technology and Computer Science, (ITCS 2009)*, 2009, pp. 472–475. [Online] Available: https://dx.doi.org/10.1109/ITCS.2009.103

[11] A. Perrig, D. Song, R. Canetti, J. D. Tygar, B. Briscoe, "Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction", Tech. rep., Carnegie Mellon University, IBM, University of California, Berkeley, BT, USA, 2005. [Online] Available: http://tools.ietf.org/html/rfc4082

[12] T. Vanek, M. Rohlik, "Analysis of broadcast authentication mechanism in selected network topologies", *Radioengineering*, vol. 20, no. 1, pp. 167–173, 2011. [Online] Available: https://dx.doi.org/10.2298/CSIS110227057Q

[13] T. Vanek, M. Rohlik, "Model of DoS resistant broadcast authentication protocol in colored Petri net environment", in *Proc. 17th Int. Conf. Systems, Signals and Image Processing, (IWSSIP 2010)*, Rio de Janeiro, Brazil, 2010, pp. 264–267. [Online] Available: https://dx.doi.org/10.1145/1288107.1288118

[14] N. Aslam, W. Robertson, W. Phillips, "Performance analysis of WSN clustering algorithms using discrete power control", *IPSI Trans. Internet Research*, vol. 5, no. 1, pp. 10–15, 2009.

[15] M. Achir, L. Ouvry, "Power consumption prediction in wireless sensor networks", in *Proc. 16th ITC Specialist Seminar on Performance Evaluation of Wireless and Mobile Systems*, 2004. [Online] Available: https://dx.doi.org/10.1.1.60.1065

[16] D. Chee, M. Suk Kang, H. Lee, B. C. Jung, "A study on the green cellular network with femtocells", in *Third Int. Conf. Ubiquitous and Future Networks, (ICUFN 2011)*, 2011, pp. 235–240. [Online] Available: https://dx.doi.org/10.1109/ICUFN.2011.5949168

[17] D. Di Zenobio, M. Celidonio, L. Pulcini, A. Rufini, "An integrated access network infrastructure combining femtocells to existing cabled networks", in *Wireless Telecommunications Symposium, (WTS 2011)*, 2011, pp. 1–5. [Online] Available: https://dx.doi.org/10.1109/WTS.2011.5960880

[18] FREEDOM, Femtocell-based network enhancement by interference management and coordination of information for seamless connectivity, Specific Targeted Research Project of the 7th Framework Programme, 2011. [Online] Available: http://www.ict-freedom.eu

[19] K.-J. Tsao, S.-C. Shen, T.-C. Hou, "Location-dependent power setting for next generation femtocell base stations", in *IEEE Wireless Communications and Networking Conf., (WCNC 2011)*, pp. 767–772. [Online] Available: https://dx.doi.org/10.1109/WCNC.2011.5779229

[20] T. Vanek, M. Rohlik, "Alternative protocols for femtocell backbone security", in *4th Joint IFIP Wireless and Mobile Networking Conf.*, NJ, USA, 2011, pp. 1–4. [Online] Available: https://dx.doi.org/10.1109/ WMNC. 2011.6097239

[21] K. R. Wadleigh, I. L. Crawford, *Software optimization for high performance computing: creating faster applications*. Prentice Hall, 2000.