Security Architecture for the Distributed Environments

Jozef Filipek*
Institute of Computer Engineering and Applied Informatics
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava
Ilkovičova 3, 842 16 Bratislava, Slovakia
jozef.filipek@stuba.sk

Abstract

Mobile ad hoc networks (MANET) have been subject of an active research for the last decade. As opposed to the wired networks, MANETs have dynamic topology, limited resources, limited bandwidth and are usually deployed in emergency scenarios outside, where landscape plays important role. MANETs are susceptible to insider and outsider attacks and bring new security challenges which were not present in the wired networks due to the individual nodes of MANETs acting like full-fledged routers. Security of the MANETs usually focuses on some key aspect of the networks, i.e. securing routing protocol, IPS (Intrusion Prevention System), trust infrastructure or secured data transfer. Current published works focused on the security lack top-down approach which would go in depth and tried to cover as much of the network as possible. This work deals with the design of a novel approach to secure MANETs by introducing several security mechanisms at the same time to create novel Security Architecture for these networks. In this paper we introduce Architecture comprised of PKI (Public Key Infrastructure), secured routing protocol, firewall and IPS. Tying all those aspects together creates viable security system for MANETs achieving level of security we are aiming for. Part of the paper are performance measurements of the deployed solution.

Categories and Subject Descriptors

C.2.0 [**Computer-communication Networks**]: General - Security and protection (e.g. firewalls); C.2.1 [**Computer-communication Networks**]: Network Architecture and Design - Network communications; C.2.5 [**Computer-communication Networks**]: Local and Wide-Area Networks - MANETs; C.4 [**Performance of systems**]: Performance attributes

*Recommended by thesis supervisor: Assoc. Prof. Ladislav Hudec
To be defended at Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava on [to be specified].

Keywords

AES, Firewall, Intrusion Prevention System, Mobile ad hoc networks, Public key Infrastructure, RSA, Secured routing protocol

1. Introduction

MANETs are dynamic, self-configuring, mobile and easy to deploy devices. Comparing it to the wired networks, they do not need fixed infrastructure with the central point (router) and each MANET node expands network's reach and adds another computing resource into the network. However, almost every advantage these networks have over wired networks can be exploited and brings forth new security challenges that are not present in wired network scenarios. Shared medium is susceptible to various threats. It can be easily eavesdropped and there are many ways to disrupt wireless communication. Disrupting at the physical layer is almost impossible to protect against and will not be in covered within our scope. Mobility of the nodes brings another security concern. It may divide the network if some of the nodes become unreachable and stranded nodes are easy target for an attack.

Since every node in the network acts like a router, behavior like that brings critical security challenge. What if one or more nodes gets compromised? What if some malicious outsider node gets connected into the network? Depending on the routing protocol used, one node can severely affect the way the network works. Since by default, MANETs do not use trust model, one compromised node can safely send malicious data to other nodes without any suspicion from other nodes. In this paper, we will focus our security improvements onto control and data plane. We address several layers of security vulnerabilities, such as eavesdropping, behavior of the nodes, cryptography and dynamic trust model between nodes. More details will be in the following chapters.

1.1 Related Work

During our research, we encountered many papers focusing on the security of the MANETs. We were focusing our attention on IPS, Firewall and distributed security systems. Major categories of these works are: Intrusion Prevention Systems (IPS) [12] [4] [19] [14] [5] [3], Secured Routing Protocols [1] [18] [16] [24] [15] [22] [11] and Securing aspects of the MANETs, meaning, different mechanisms to protect networks against specific attacks, for example DoS (Denial of Service) or routing attacks. The least amount of papers was focused on the firewall systems because of the nature of the MANETs [23] [20] [21]

[10] [17]. We've also covered solutions focusing on introducing whole security architecture for MANETs [13] [2] [8] [6] [7], but all of them have some flaws or they are not design to cover as security of the network as much as we aim to do.

Based on our analysis of existing solutions and previous work with the security in MANETs, we decided to use existing PKI with secured routing solution developed in our department [9] and on top of it we are adding custom Firewall solution while simultaneously some nodes act like IPS.

2. Thesis Objective

The central thesis of this dissertation is to design, implement and test security architecture for MANETs securing the network as much as possible using existing and newly proposed mechanisms to achieve required level of security.

In order to fulfill the main thesis, following objectives have been defined:

- Propose security model for distributed environment spanning several layers OSI. Under the term security we understand deploying confidentiality, integrity and authentication into the network. Achieving this objective will require proposal of several mechanisms required to secure behavior of mobile networks in the distributed environment:
  - Verification of node's identities
  - Authorization of services in the network
  - Distributed control of authentication and authorization in the network
  - Securing of traffic at different OSI layers
  - Distributed behavior control in the network
- Verify proposed security mechanisms, approaches, realized solutions and used methods through analytical model and testing in network simulator environment.

  Scientific contribution of the dissertation lies in the detailed proposal of the new security architecture for mobile distributed environments, its verification and evaluation. Our proposed security architecture consists of several security mechanisms which will be interleaved and cooperating witch each other.

3. Specifications

Based on our analysis, experiences and thesis objectives we have defined specification defining our proposal of the security architecture:

- Utilize verified and reliable mechanisms and approaches
  - From the point of building network security, it is more efficient and better to use existing mechanisms and approaches, or modify them to satisfy our requirements
- Ensure integrity and authenticity of transmitted control and data traffic
  - Ability to verify and police all control traffic is absolute foundation for a secured solution
  - Part of control traffic verification is to verify origin of the traffic and its reliability
  - Same conditions as above apply for data traffic
- Control traffic confidentiality
  - This requirement is not absolute. Confidentiality in wireless networks has to be approached a little different since other nodes will lose visibility to the traffic and depending on the deployed solution it may not be desirable.
- Data traffic confidentiality
  - Requirement is to confidentially secure as much data traffic as possible, ideally all.
- Keeping network homogeneous.
  - To lower the chances of discovering important nodes in the network, all nodes should look to the outsiders the same.
  - This requirement makes it harder for the attacker to pick and compromise crucial nodes in the network.
- Node behavior control.
  - Bandwidth
  - Services
  - Alarms
  - Malicious behavior
- Decentralized behavior
  - Diminishing single point of failure by distributing security functions onto several nodes
- Granularity of access rights in the network
  - Different levels of authorization for the nodes

4. Proposed Solution

This section covers our security model for MANETs and gives high-level overview how the solution works, what parts it consists of and security impact it has on the network. Main difference from the analyzed solutions is scope of deployed protection onto the network. We do not cover only security protocol, part of the behavior or some different aspect of the security. Our aim is to cover the network as much as possible and thus introducing security architecture consisting of secured routing protocol, trusted public key infrastructure, per-node firewall and IPS. This covers not only confidentiality, integrity and authentication, but also partial behavior of the network. Not all secured members of the network execute same security functions at the same time.

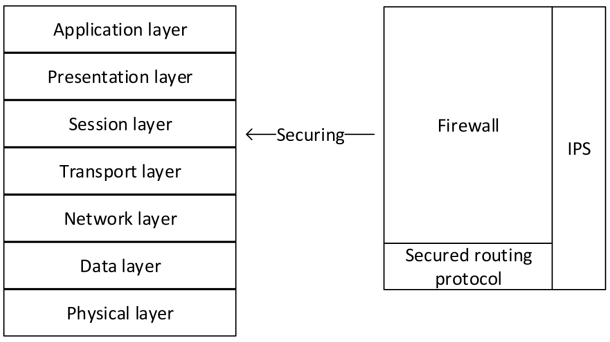

Figure 1: OSI layers to security architecture

4.1 Security Architecture

As mentioned before, complex security architecture requires securing control and data plane and behavior of the network. Control plane consists of routing protocol, firewall and IPS. End-to-End communication is treated as data plane. Figure 1 depicts how layers of proposed architecture corresponds to OSI layers.

Per our goals, we are not trying to secure physical layer as that would in most cases require specially modified transfer medium. Routing protocol (BATMAN) operates at the data layer and every packet is signed by sender. Due to the deployed PKI which operates at the same layer as the routing protocol and utilizes it for its function, there is already trust model present and every node is capable of control traffic verification. Since every packet sent has routing protocol header, whether it is control or data packet, nodes are able to verify integrity and authenticity of every packet.

Network and upper layers are secured via firewall. Every node participating in the network communication has attribute certificate thanks to the PKI and firewall further extends use of attributes in the certificate. When two nodes want to communicate with each other, they are going through the process of exchanging session certificates, which are similar to attribute certificates, only these do not assign identity to the nodes but their main purpose is to define capabilities which will be used in the subsequent communication. Session certificates are signed using private keys, but their content is not encrypted even though deployed infrastructure allows this possibility. Capabilities negotiated contain allowed bandwidth, services and shared secret. Shared secret is computed via DH (Diffie-Hellman) algorithm and is used for encrypting data communication. Since it is known only to the pair of nodes, we are not using it for packet signing. Even though it would be less CPU intensive, nodes not possessing secret would not be able to verify signature on the packets they receive. Sender defines how much bandwidth and what services it would like to use, but final decision goes to the receiver which calculates what capabilities will allow based on its own circumstances and replies back to sender. Sender has to accept whatever capabilities receiver defines.

Figure 2 depicts data packet in the network based on OSI layers and security mechanisms. From routing protocol higher, the packet is signed by sender's private key. All data from the network layer higher is encrypted with shared key. Firewall part is not encrypted so other nodes can verify capabilities and act accordingly.

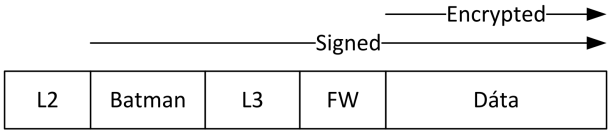

Figure 2: Secured data packet

4.2 Public Key Infrastructure

What is fundamental for the security is having trust model deployed in the network. That is why we have decided to use existing solution proposed at our faculty [9]. It brings to the network trust model along with PKI and it uses underlying secured protocol for transit. Our architecture proposal required some minor changes to the approach, namely we changed number of privilege levels and modified certificates handed by Attribute Authorities (AA). Trust model divides nodes into several authorization levels:

- Implicit authorization - nodes do not have any certificates, nor access rights, they are not part of the secured infrastructure
- L1 - basic access rights, not authorized to participate in the routing protocol decisions, only allowed for end-to-end communication
- L2 - participates in routing decisions, forwards network joining messages from other nodes to the AA, fully integrated node
- L2s - same as L2, but is also part of distributed IPS and certification storage, fully integrated node
- L3 - role of AA, capable of escalating privileges to the nodes, in case of L3 escalation, another ecosystem is created and cross-certification takes place with the AA, part of distributed IPS and certification storage

4.3 Firewall layer

As specified in the specification, data are supposed to be encrypted with shared secret and during session negotiation, network constrictions for node's communication are defined. All this happens after nodes have routing connection between each other, i.e. their identity can be verified and are part of the trust model in the network. Following subsections will provide basic view as to how the firewall part works.

4.3.1 Firewall certificates

Control plane of the firewall uses two certificates. Forward and session certificate. *Forward certificate* is utilizing underlying PKI and is part of the attribute certificate in the form of attributes. Attributes define allowed communication radius and services for the node. All those depend on the deployed infrastructure and have to be pre-configured before or during deployment. *Forward certificates* are negotiated before data transfer when nodes want to communicate with each other. Semantics of the certificate are similar to that of X509.3, but slightly changed, since we do not need to define in this step node's identities, only transport attributes.

Session certificate transfer can be secured using few options. All have their pros and cons. One would be to encrypt the whole session certificate with present public key

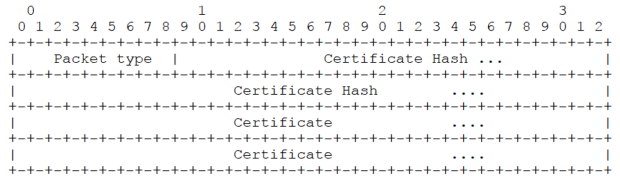

Figure 3: `FW_SES_EST and FW_SES_RES packet`

of the receiver, but that would mean other nodes could not police traffic based on the negotiated requirements. Even though this option looks as most secured, it brings forth drawback which could potentially diminish security of the network by losing capability of other nodes to verify passing traffic. Second option would be to encrypt shared secret with public key and send it to the receiver. This option would not require DH calculation and it would still be secured. The last option is to use the DH to compute shared secret and that is the option we chose. Please note, that thanks to the routing protocol all packets are at this point signed. We decided for this option because transport attributes negotiated via session certificates require sending two packets and this option produces a little less overhead compared to encrypting shared secret with the RSA.

4.3.2 Control messages

For our architecture we proposed and implemented several control messages. Their purpose is to deal with session negotiation, missing certificates and data transfer encapsulation.

- `FW_SES_MIS` (Firewall Session Missing) - When node is missing session certificate necessary to verify passing communication, this request is sent.
- `FW_SES_RES/FW_SES_EST` (Firewall Session Response / Establish) - Responsible for firewall session negotiation and answer to the node missing the certificate (Figure 3).
- `FW_DATA` (Firewall Data) - Defines firewall header for the data packet identifying its session.

All control messages are identified by the field *Packet type* and individually signed by their each originator.

4.3.3 Communication Model

In this subsection we will describe how the session negotiation and subsequent data transfer work at the firewall layer. Situation before this negotiation is that all secured nodes possess each other certificates and the routing is working in the network. Figure 4 depicts communication exchange we will be describing. We also cover possible movement in the network when there is a new node which has not received session certificate identifying the communication. Intermediate nodes are part of the secured network and their only activity in this scenario is to forward traffic to the destination.

1. Requesting permission to communicate end-to-end and sending Establish message.
2. Verifying message by intermediary node. If successful, message gets forwarded.

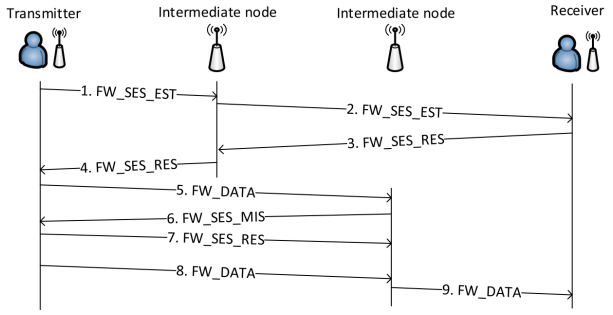

Figure 4: Session creation and data transfer at the firewall layer

3. Processing the communication requirement and sending response message. Computing shared secret.
4. Same as 2nd step.
5. Processing response message. Movement takes place in the network and path between Transmitter and Receiver changes. Transmitter sending data communication.
6. Receiving encrypted data with session certificate not in the database. Requesting missing session certificate from the node the data packet was received.
7. Sending requested certificate to the requester.
8. Verifying communication and forwarding it.
9. Receiving, processing and decrypting packet.

4.4 Intrusion Prevention System

Secured routing protocol and firewall bring elevated security into the network, but it is still not enough for effectively covering the whole security. IPS is necessary to dynamically protect the network against inside and outside attack. Currently, this work does not cover complete stand-alone IPS solution. Implemented were only parts that cover against violating network constraints, but in the future we expect architecture to contain full-fledged distributed IPS which has following functions:

- Identification of Blackhole, MitM and Sybil attack
- Every entry has defined source in the storage
- Policing of the network constraints identified in the attribute and firewall certificates
- Certificate revocation in case of violating network policies
- Keeping up with communication flows in the network and creating security profiles for each node
- Synchronization of the IPS entries with distributed storage

4.5 Overall Security of the Proposal

Proposed architecture is secured against following attacks:

- Spoofing of the routing information
- Eavesdropping of data communication between nodes

- External node's attacks on the secured network
- DoS attack of the compromised nodes on the rest of the network
- Attacks of the compromised nodes on the rest of the network violating constraints

Distributed PKI along with its routing protocol protects against lower layer attacks, specifically it is resistant against routing protocol attacks. Every node has its own certificate and certificate of the AA. In case of cross-certifications, nodes obtain certificates of other AAs. That gives us working trust model in the network in the form of PKI. Nodes are able to verify each other identities. Not only that, but due to the deployed L2 routing protocol every message sent through the network is signed by the sender and also verifiable. Trust model is enhanced by dividing node's access right into several categories. Newly joined participants do not participate in the routing decisions, after some time they can request AA to escalate their privileges. By delaying escalation of access rights nodes become less attractive for attackers to compromise.

Firewall layer protects network above routing protocol and enforces nodes to comply with dynamic policies created during session establishment. As described in the previous section, pair of communicating nodes goes through a process of session establishment before they can forward data packets between each other. During the session establishment, nodes compute shared secret with DH algorithm and negotiate network constraints on the subsequent communication. Secret is used to encrypt data traffic, since it is more viable solution than using RSA because of processing requirements. Constraints serve to limit traffic based on the bandwidth or used services. They are also used by other nodes to actively verify traffic and in case of the violation, IPS will be notified. Worst case scenario is revocation of the node's certificate.

Any communication not belonging to the secure part of the network is automatically denied. Nodes which do not possess its own certificate are considered security risk and the only communication allowed with them is to grant them L1 rights. In case of malicious nodes, situation is more complicated. When nodes start to perform DoS attack and clearly violate communication restrictions, it is easy to detect them and revoke their certification. Other case is when they do not violate conditions and start to steadily exhaust resources of the network. In this case, even with fully operable IPS, it will be difficult to discover intrusion and shut it down.

5. Evaluation

We evaluated proposed solution in the OMNET++ simulation environment with a known library INET.

Goal of the experiment was to determine if additional overhead incurred by cryptographic operations was feasible to maintain normal operation of the network. We performed evaluation of known cryptographic algorithms on different configurations. In the simulations we used the results from the slowest configuration (Rapsberry Pi - 900MHz, 1GB RAM) which is comparable to current low-end mobile devices. As our initial topology to compare baseline of unsecured network and our architecture

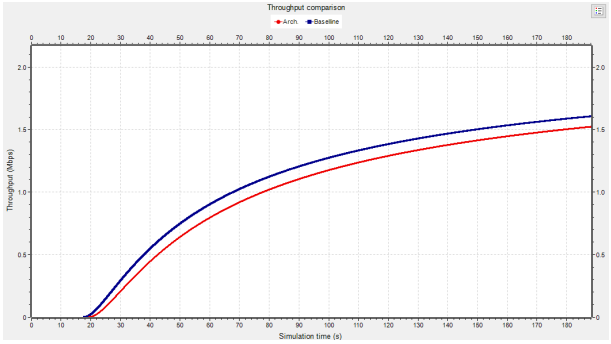

Figure 5: Comparison of the end-to-end delay between baseline and architecture

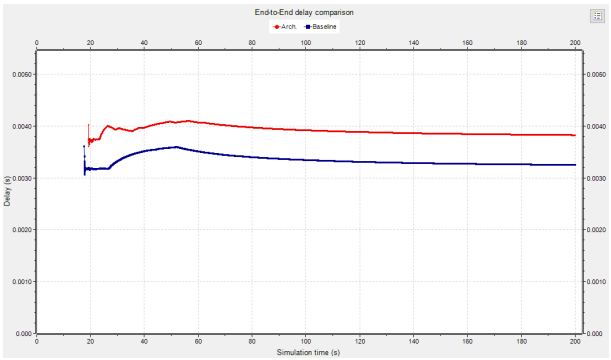

Figure 6: Comparison of the throughput between baseline and architecture

we decided to use line topology, also present in the analyzed solutions. Encryption algorithms in our solution are AES 128b, SHA 256 and RSA 1024b.

Simulation results in the Figure 5 and 6 depicts comparing of end-to-end delay and throughput of baseline and architecture. Distance between nodes is 6 hops and we can see the difference between secured and unsecured network. We used UDP flow using 1350B of data, sent every 0.005s. Maximum theoretical throughput of this flow is 2.18Mbps at the application layer. Throughput computation used formula to take into consideration whole sending time, that is why it has ascending nature. Maximum throughput achieved by unsecured network is 1.6Mbps, architecture was able to get to the value of 1.5Mbps. End-to-end delay is 0.0032s for the unsecured network, 0.0038s for the architecture. We can see that architecture causes 5-10% higher delay and about that value worsened delay.

6. Conclusion and Contribution

In this work we present our proposal of security architecture for MANETs. We utilize existing and new security mechanisms to achieve our required level of protection. The presented solution uses secured routing protocol, PKI, firewall and IPS. All these components work with each other and ensure the network is protected as much as possible. Routing protocol works at Layer 2 and is used for the PKI. All messages are signed and can be verified. Firewall takes on novel approach since there were needed conditions to take into account while deploying it into mobile networks. IPS is able to police network based on the constraints brought upon by the PKI and firewall. Proposed architecture has been implemented in the network simulator environment and performance evaluations

took place. We compared unsecured and secured network to verify feasibility of the proposed solution. Results were very promising and network operation was only partially affected. Overall operation of the network was worse up to 10%.

The contribution of this work is the development of a novel approach to secure MANETs with complex security architecture using several elements. Compared to existing proposals, the main difference between them and our solution is the scope of the security imposed onto the network. None of the other approaches used secured routing protocol, trust infrastructure, firewall and IPS.

Acknowledgements. This work was partially supported by research grants VEGA 1/0722/12, VEGA 1/0774/16, Programme for supporting young researchers, and Eset Research Centre.

References

[1] L. X. a. L. K. A. Boukerche, K. El-Khatib. Sdar: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks. *29th Annual IEEE International Conference on Local Computer Networks*, (6):618 – 624, December 2004.

[2] T. N. a. C. M. K. Plossl. Towards a security architecture for vehicular ad hoc networks. *First International Conference on Availability, Reliability and Security*, page 8, April 2006.

[3] D. W. a C. Scott. Methodology for evaluating the effectiveness of intrusion detection in tactical mobile ad-hoc networks. *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, 1(5):622 – 627, July 2004.

[4] V. T. a. A. K. A. Chaudhary. Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks. *Advance Computing Conference (IACC), 2014 IEEE International*, November 2014.

[5] S. U. a D. Naik. Anomaly based intrusion detection of packet dropping attacks in mobile ad-hoc networks. *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on*, pages 1137 – 1140, July 2014.

[6] S. J. E. T. a. G. G. S. Darwish. Security server-based architecture for mobile ad hoc networks,. *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, March 2012.

[7] Y. W. a. J. H. H. Wang. Security architecture for tactical mobile ad hoc networks. *Second International Workshop on Knowledge Discovery and Data Mining*, July 2009.

[8] X. Y. a. J. Li. A security architecture based on immune agents for manet. *International Conference on Wireless Communication and Sensor Computing*, (5):1 – 5, January 2010.

[9] P. V. a L. Hudec. Building public key infrastructure for manet with help of b.a.t.m.a.n. advanced. *Modelling Symposium (EMS), 2013 European, Manchester*, July 2013.

[10] H. Z. a S. Bellovin. High performance firewalls in manets. *Mobile Ad-hoc and Sensor Networks (MSN), 2010 Sixth International Conference on*, (6):154 – 160, December 2010.

[11] L. Z. a S. Shudong. A secure routing protocol for mobile ad hoc networks. *Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on*, (5):153–157, July 2007.

[12] R. B. a X. Su. On the effectiveness of monitoring for intrusion detection in mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 10(12):1162 – 1174, November 2011.

[13] Y. H.-L. a. Z. Q.-S. L. Shi-Chang. Research on manet security architecture design. *International Conference on Signal Acquisition and Processing*, pages 90 – 93, February 2010.

[14] Y. X. a. S. G. B. Sun, L. Osborne. Intrusion detection techniques in mobile ad hoc and wireless sensor networks. *IEEE Wireless Communications*, 14(7):56–63, December 2007.

[15] D. M. a. H. M. B. Vaidya. Provisioning secure on-demand routing protocol in mobile ad hoc network. *2011 Second Asian Himalayas International Conference on Internet (AH-ICI)*, (5):1 – 5, November 2011.

[16] L. Q. a. A. K. I. Khalil, S. Bataineh. Distributed secure routing protocol for mobile ad-hoc networks. *Computer Science and Information Technology (CSIT), 2013 5th International Conference on*, (5):106 – 110, March 2013.

[17] L. H. J. Filipek. Distributed firewall using pki in mobile ad hoc networks. *2016 IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, (5):321 – 325, January 2015.

[18] D. L. a. H. Z. L. Jin, Z. Zhang. Implementing and evaluating an adaptive secure routing protocol for mobile ad hoc network. *2006 Wireless Telecommunications Symposium*, (10):1–10, April 2006.

[19] R. A. a. A. K. L. Rajeswari. Information and communication technology in electrical sciences (ictes 2007), 2007. ictes. iet-uk international conference on. *ACM Trans. Program. Lang. Syst.*, (5):1008–1013, November 2007.

[20] K. A. D. A. M. Diploma: Distributed policy enforcement architecture for manets. *Network and System Security (NSS), 2010 4th International Conference on*, (10):89 – 98, September 2010.

[21] A. K. a. A. S. M. Alicherry. Evaluating a collaborative defense architecture for manets. *2009 IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, (6):1 – 6, December 2009.

[22] H. J. a. M.-K. K. N. V. Vinh. A self-secure routing protocol for large mobile ad hoc networks. *Wireless and Optical Communications Networks, 2007. WOCN '07. IFIP International Conference on*, (5):1 – 5, November 2007.

[23] I. Z. a. M. I. S. Akram. Fully distributed dynamically configurable firewall to resist dos attacks in manet. *Networked Digital Technologies, 2009. NDT '09. First International Conference on*, (3):547 – 549, July 2009.

[24] R. C. a. N. C. S. Saha. A new reactive secure routing protocol for mobile ad-hoc networks. *2008 7th Computer Information Systems and Industrial Management Applications*, (5):103 – 108, June 2008.

Selected Papers by the Author

J. Filipek, L. Hudec. Distributed firewall using PKI in mobile Ad Hoc networks *CompSysTech'15. Proceedings of the 16th International Conference on Computer Systems and Technologies CompSysTech '15, Dublin, Ireland* June 25-26, 2015 New York: ACM, 2015, s. 292–298. ISBN 978-1-4503-3357-3

J. Filipek, L. Hudec. Distributed firewall in mobile ad hoc networks. *SAMI 2015. IEEE 13th international symposium on applied machine intelligence and informatics*, January 22-24, 2015 Herlany, Slovakia: proceedings. 1. vyd. S. l.: IEEE, 2015, s. 233–238. ISBN 978-1-4799-8221-9.

J. Filipek, L. Hudec. Advances In Distributed Security For Mobile Ad Hoc Networks In *CompSysTech 2016. Proceedings of the 17th International Conference on Computer Systems and Technologies 2016*, 23-24 June 2016, Palermo, Italy. 1. vyd. New York: ACM, 2016, s. 89–96. ISBN 978-1-4503-4182-0.

J. Filipek, L. Hudec. Securing Mobile Ad Hoc Networks Using Distributed Firewall with PKI. *SAMI 2016: IEEE 14th international conference Symposium on Applied Machine, Intelligence and Informatics*, Herlany, Slovakia, January 21-23, 2016. 1. vyd. S. l.: IEEE, 2016, s. 321–325. ISBN 978-1-4673-8739-2.