International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 2 December 2019

Security Architecture for MANETs

[1]Kholilah Hilaluddin, [2]Mohd Zhafri Mohd Zukhi
[1]School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia
[2]Universiti Teknologi MARA, 08400 UUM Sintok, Merbok, Kedah, Malaysia

Abstract: For the past several years, mobile ad hoc networks (MANETs) security has been an ongoing research subject. MANETs have diverse topology, limited resources, restricted bandwidth, as opposed to wired networks, and are typically implemented outside in emergency situations where landscape plays an important role. MANETs are vulnerable to insider and intruder attacks and carry with them new security problems not present in the wired networks. The main difference is that each node in MANET serves as a network-wide router and routes traffic. Compromising a single node can have a major impact on network performance. We present our security architecture for MANETs in this paper that secures important network aspects. We take the concept of trust into the network and nodes are protected by various mechanisms specifically tailored for use in the distributed environment. We use OMNeT+ to simulate networks. Analyses use delays measured on the actual hardware and we examine network performance during various loads on the data plane and the control plane.

Keywords: AES, attribute authority, architecture, firewall, MANET, PKI, RSA, security

I. INTRODUCTION

Advancements in mobile devices including higher computing power, low energy usage and increased internal storage make it more possible for them to take part in the network's vital roles. Typically, mobile devices are and have been used as end devices, but nowadays they are increasingly capable of making up the internal part of the network. MANETs are tools that are flexible, self-configuring, mobile and simple to use. We do not need a fixed infrastructure compared to the wired network works with the central point (router) and each MANET node extends network scope and adds another computing asset to the network. Nonetheless, it is possible to exploit almost every advantage these networks have over wired networks and bring new security challenges which were present in wired network scenarios. There are several other threats to the shared medium. It can be easily eavesdropped and wireless communication can be disrupted in many ways. It is almost impossible to protect against disruption in the physical layer and will not be covered within our scope. Node mobility brings with it another security concern.

It can break the network when one of the nodes is unattainable and stranded nodes easily target the attack. Because each node in the network behaves as a router, such behavior brings with it critical security challenges. What if it compromises one or more nodes? What if the network connects to some malicious intruder node? The way the network operates can be severely affected by one node, depending on the routing protocol used. Because MANETs does not use trust model by default, one compromised node can safely send malicious data from other nodes to other nodes without any suspicion. In this article, we will concentrate on monitoring and data plane for our security improvements. We approach multiple layers of vulnerabilities within security, such as eavesdropping, node actions, cryptography, and dynamic node trust model. The following chapters will provide more information.

II. RELATED WORK

We found several papers focusing on the security of the MANETs during our study. We concentrated on IPS, Firewall and centralized security systems. Main categories of these works are: Intrusion Prevention Systems (IPS)[4][11][13][20], Secured Routing Protocol [5][9][12][15][19] and Securing elements of MANETs, meaning different network security mechanisms towards specific attacks, such as DoS (Denial of Service) or routing attacks. Due to the nature of the MANETs [1][2][3][21], the least amount of papers were based on the firewall systems.

Depending upon our review of existing solutions and earlier work on protection in MANETs, we planned to use existing PKI with a protected routing system built in our [16] department and include custom firewall solution.

III. SECURITY ARCHITECTURE

As described above, together with PKI, Firewall and IPS, our solution consists of a secured routing protocol. All elements interact and use the same information sources. At the lowest layer, together with PKI, we use secure BATMAN routing protocol. In contrast, our Firewall solution is in terms of network layers. IPS enforce policy among all PKI and Firewall nodes. We're trying to solve

Copyright © 2019 Mélange Publications

the following vulnerabilities in MANETs with this architecture:

- Node trust
- Communication confidentiality and integrity
- Dynamic node behavior changes

We decided to use hashing function SHA-512, asymmetric algorithm RSA with key length of 1024b and symmetric algorithm AES with key length of 128 bits based on our analysis, simulation and measurements.

A. Public Key Infrastructure with Secured Routing Protocol

It's where we place inspections and trust models. Our solution uses protected BATMAN protocol version and PKI model that interacts with the routing protocol. It acts as our solution's safety underpinnings. The trust model uses 4 node rights (L0 L3) level. L0 nodes are considered and in no way trusted as outsider nodes. The only activity they are allowed to do is to ask the AA (Attribute Authority) for the certificate. They become L1 nodes after they receive the certificate. End-to-end communication within the network is permitted for L1 nodes. However, they are not allowed to participate in the routing as the preventative and security measure. It makes strangers less risky in the network and it is not possible to originate the attack from the location of the attackers. They can demand to lift their privileges to L2 after some time and when nodes behavior complements with network policies.

L2 is involved in routing, storage distribution, and IPS. It can revoke certificates locally depending on the irregularities in the network, i.e. it does not permit misbehaving nodes to be communicated by itself and generates alarm about them, which goes to other nodes L2 and L3. L2 nodes may request that their privileges be elevated to L3 after sufficient time and clean policy history. L3 is a stand-alone AA that can certify other nodes. Each AA creates its own ecosystem, that is, nodes with certificates from that AA.

Two AAs create 2 different ecosystems and need cross-certification for them to interact with each other. Ecosystems can interact with one another in this way.

BATMAN is modified and secured using a RSA algorithm using 1024-bit public / private keys. AA is responsible for distributing certificates of attributes to individual nodes. Certificates are signed by AA and each node with AAs public key can verify the validity of the certificate.

Certificates have finite validity and nodes need to ask their AA to recertify them when their validity is about to expire. BATMAN has new and modified control messages to work with this modification. Crt request and crt response for the request and answer of the missing node certificate and updated BATMAN protocol message for PKI and multiple ecosystems use, Fig.1 to 3.

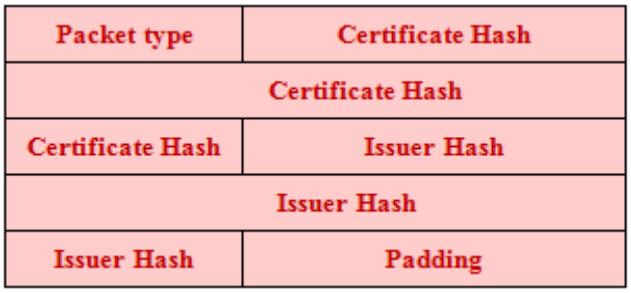

Figure 1. BATMAN crt request control message

Figure 2. BATMAN crt response control message

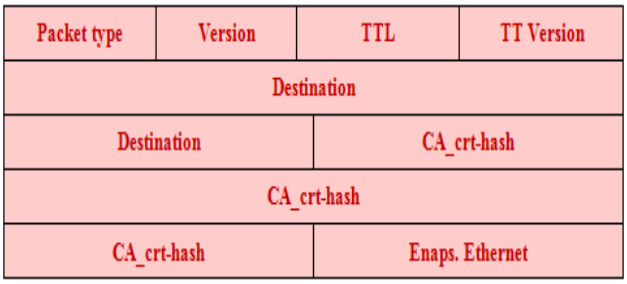

Figure 3. BATMAN packet with encapsulated data

Each BATMAN message is signed by the respective private key senders and it is require for all nodes that communicate with each other to have certificates for signature verification to be successfully processed.

B. Firewall

Firewall is used in our software as a security overlay. This includes protection of the rule of privacy and information sharing. This chapter will explain how exactly this conducts its operations. Normally, firewall is installed in the network at an entry point and all contact between the outside and the inside of the network should go through it. This is almost impossible to use this idea in MANETs. Since every node routes traffic and even if we were to restrict interaction in the network via many specially chosen nodes, because of the complexity of MANETs, it wouldn't be a very viable solution. We chose to use another strategy. We concluded our Firewall needs to meet several requirements based on our earlier work and simulations:

- Initial Firewall Policy Deployment
- Defined attributes and certificates
- Secure data privacy exchange of mutual secrecy

Copyright © 2019 Mélange Publications

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 2 December 2019

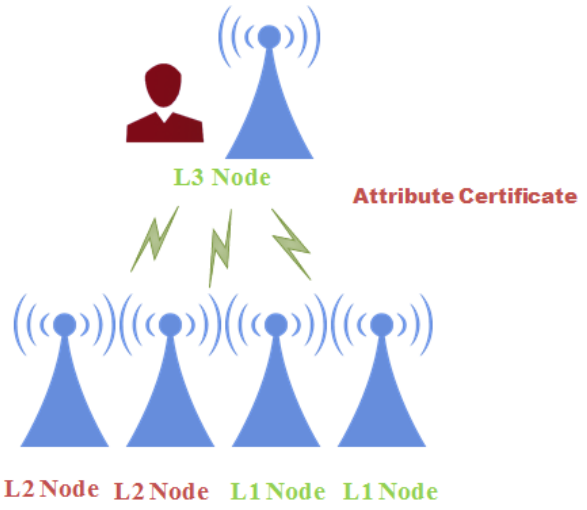

Figure 4. Handing out certificates during creation of the network

- Used data storage
- Communication message control
- Communication model

Initial deployment of the firewall policies

Each node contains the mechanism of the firewall and can control other nodes except nodes L0 and L1. This is done through special attributes that can finite the nodes used bandwidth, their radius of communication, and the services they can use. Initial attributes are included in the AAs certificate. Almost every node can see them and, based on their values, can police the communicating node. Figure 1 shows the AA's issuance of certificates. They also contain the FW attributes required for police traffic.

It's the only unsecured part of our architecture's correspondence. It is vulnerable to attacks by MITM (Man in the Middle) and eavesdropping. In the communication, the only possible way to protect this step would be to do it with the certificates in the controlled environment or preload nodes.

Defined attributes and certificates

Attributes with the following semantics are specified in the node attribute certificate:
Destination FC: aa** / Communication radius
Service FC: 3 / Allowed services
Bandwidth FC: 3 / Maximum allowed bandwidth in multiplications of 64 kbps
Secondly, for other nodes, we needed some form of more granular and dynamic control. This is accomplished by certificates of training. Next to their semantics:
Serial Number SC: 130745 / Session ID
Issuer SC: Aaaa / Certificate owner
Subject SC: aaaa / Communication radius
Validity SC: 2013-10-25 / Certificate validity
Service SC: 3 / Allowed service
Bandwidth SC: 10 / Allowed bandwidth
signature SC: sig-rsa 23455656 / Signature
The negotiation of certificates is mentioned in the chapter below.

Secured exchange of the shared secret for data confidentiality

Permitted bandwidth is sufficient for creating session certificates in the attributes of the attribute certificate. A session certificate is created when node wants to communicate end-to-end with some other network node.
Session certificates depend on RSA and each node already has RSA key pair allocated at this level in the communication. Figure 5 demonstrates the existence of session certificates together with the creation of shared secrets. We utilize the DH algorithm to measure shared secrets securely. Session certificates were only valid for a limited time period and only for the nodes chosen. Nodes can demand more bandwidth for subsequent data communication over this exchange.
As shown in Figure 5, the transmitter may demand more bandwidth than allowed by the receiver. The receiver has the final word and the decision must be approved by the transmitter. Decision is based on the use of currency rent (CPU, memory, and bandwidth) receivers.

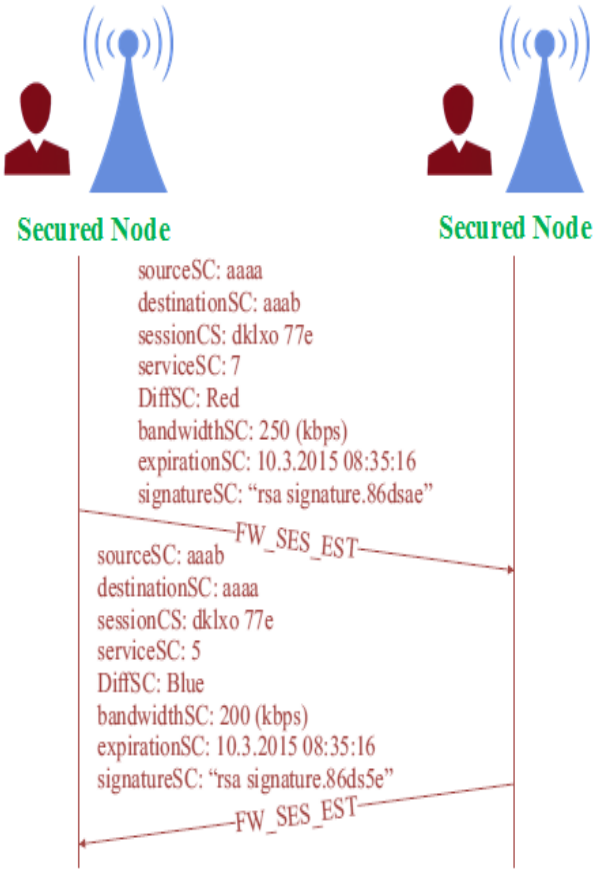

Figure 5. Session certificate establishment

Copyright © 2019 Mélange Publications

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 2 December 2019

Storage of the used data

Whole architecture uses same databases for its functionality:
• Certificate database
• Violation database
The database of certificates is utilized to store certificates of attributes and sessions. Any packet that thoroughly flows, the node is checked towards this database.
The violation database includes node information that violated network policies in a certain way. Either the integrity check fails, too much traffic is sent, and so on.

Figure 6. $\mathrm{fw}_s\, es_s st/\mathrm{fw}_s\, es_r espacket$

Figure 7. FW $_s\, ES_M\ Ipacket$

Figure 8. FW $_D\, ATpacket$

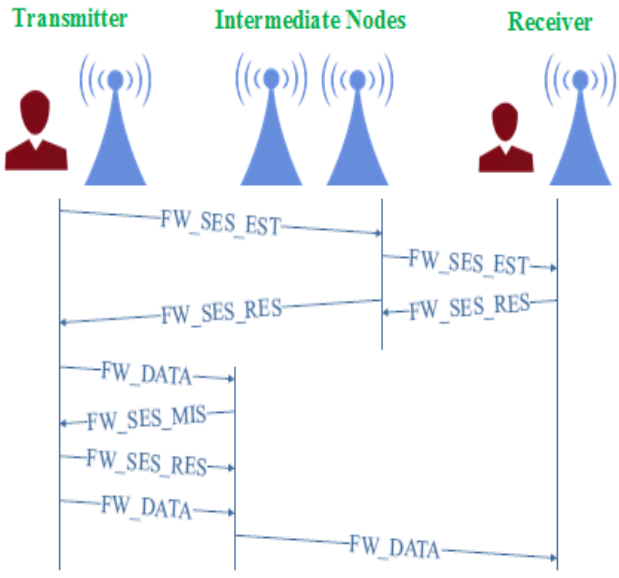

Figure. 9 Data communication

Control messages required for the communication

Depending on our study and testing, the architecture's Firewall component contains 4 control messages necessary for its smooth functionality. FW SES EST (Firewall Session Establishment) is utilized in the session certificate creation process, Figure 6.
Both sides are using the same packet structure. Contrast is only in the Packet Type area, where a receiver or transmitter sent the packet.
FW SES MIS (Firewall Session Missing) can be utilized when the session certificate of the intermediate node is missing. This packet includes the required certificate hash and the whole packet signature, see Fig. 7.
FW data (Firewall Information) encapsulates the firewall control information with the data payload.
FW Information (Firewall Information) encapsulates the firewall control information with the information payload. The only description is the Session certificate hash. Fig. 8.
It is worth mentioning that there is no asymmetric cryptography performed by the Firewall layer. BATMAN's lower-level encapsulation already signs the packets.

Communication model

Figure 9 shows the communication of data to network nodes. Initially, there is an exchange of session certificates where the shared key is calculated. Nodes can send traffic to each other securely after that.
We can see that initial exchange is moving to various intermediate nodes the subsequent interaction, which can be triggered by many factors, e.g. nodes might have moved or the radio signal has changed. When the fresh intermediate node is unaware of the session certificate contact nodes being used, the received traffic is dropped and the receiving node demands certificate. It can continue transmitting traffic among these nodes after receiving the missing certificate.
There are 3 options on how contact is done by the Firewall:

- Receiving upper layer data
- Receiving lower layer data
- Managing session certificates (i.e. Receiving, Sending and Processing)

Existing sessions are reviewed while receiving information from the top layer. When a session between nodes has already been established, the node will only encrypt the data and forward it. A session certificate is generated and sent to the receiver of the communication in the case of a completely new contact request.
Initiator and receiver manage certificates separately upon receipt of the session certificate.
The receiver reviews available resources and determines on the basis of them whether to recognize or change the specifications of the initiators. Then he is interested in his

Copyright © 2019 Mélange Publications

own DH computation, generating session certificates and submitting them to the initiator.
The initiator completes DH computation and stores certification in their server. The managing session certificates are shown in Fig.10.

C. Intrusion prevention

In our security architecture, IPS is important. This monitors nodes and ensures security policies are adhered to. Security policy consists of the principles of PKI and Firewall.
Nodes may have their licenses revoked completely or partially, depending on the severity of the crime.
PKI including routing protocol is liable for signing correspondence and ensuring that it has not been altered during transmissions, and Firewall is liable for confidential data transfer with the distribution of network restrictions that can be imposed by all relevant nodes, i.e. L2 and L3. DHT (Distributed Hash Table) propagates all warnings and events.

D. Security analysis

From the point of view of security, our architecture secures nodes with asymmetric algorithm at the routing layer, data communication is protected at the network layer and node behavior is managed by PKI, Firewall and IPS. Our strategy gives the following key points of extra security:

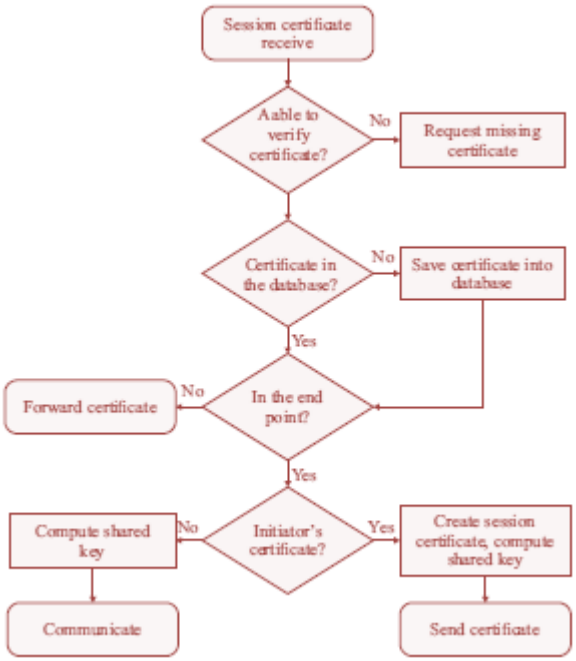

Figure 10. Session certificate handling

• Signing and checking routing and network layer interaction with RSA (due to BATMAN encapsulation application payload)
• Network layer knowledge authentication with symmetric AES algorithm
• Dividing rights into multiple groups
New nodes are not involved in the vital parts of the network: routing, intrusion detection
• Delayed node involvement in the vital tasks mentioned above makes them unattractive to attackers
• Dynamic node privileges changes
Higher level nodes (L2 and L3) police other nodes and can revoke malicious node certificates based on their IPS warnings and DHT cooperation L3 • Contact with unsecured nodes is forbidden by default • Secured nodes are constrained by their own rights and firewall restrictions.
The largest threat in the MANETs is the currently protected nodes being hacked. The greater level of privilege, the greater the threat to the network that it may pose. That's why nodes may become L3, AAs, so there would be another cross-certification among ecosystems and another AA can take over in the event of failure.

IV. SIMULATION RESULTS

In the simulation environment of OMNeT++, security architecture was introduced. To build base representation for our simulation, we used measurement of cryptographic operations on the real hardware. Quad core ARM Cortex 900MHz processor was used for these tests, which has slightly lower performance compared to current average mobile devices.
This conducted in 10s time interval 1363 RSA signs and 25994 RSA verifications. AES performed in 3s at 63895 encryptions / decryptions.

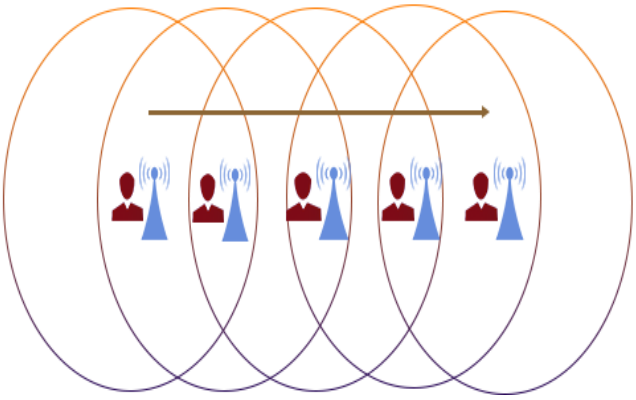

Figure 11. Line topology

The simulations performed on the topology of the line are shown below (Figure 11).
UDP CBR traffic was used for the following calculation. There were 1350B packets sent every 0.04s. Sending began at the simulation's seventh second.
Figure 12 is a packet failure based on the number of hops that have been transmitted. Failure with the protected architecture was higher than without it, which effectively

Copyright © 2019 Mélange Publications

reflects the effectiveness of the routing protocol, but stayed within acceptable limits.

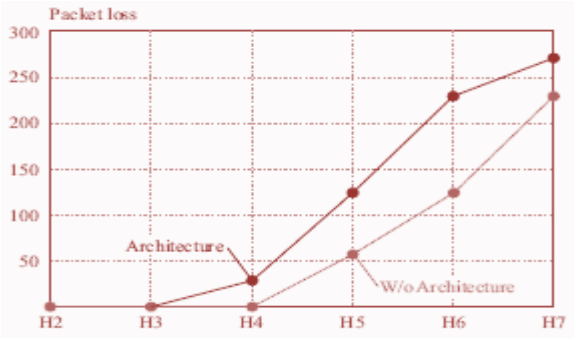

Figure 12. Packet loss

The UDP traffic output is shown in Figure 13. Throughput was also lower depending on the number of hops passed, but still within acceptable limits, and symmetric encryption did not put much pressure on the bandwidth that was usable. Figure 14 represents the number of hops depending on latency. Latency is suffering more in ad hoc networks and with the rising number of hops, we can certainly have something that is receiving much bad.

Figure 15 and Figure 16 illustrate the difference among networks that use our architecture and use a simple routing protocol without it. We will see that, due to higher overhead architecture and symmetric data encryption, there is small difference.

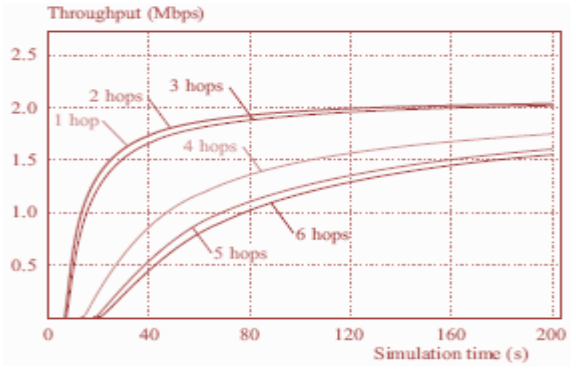

Figure 13. Architecture throughput

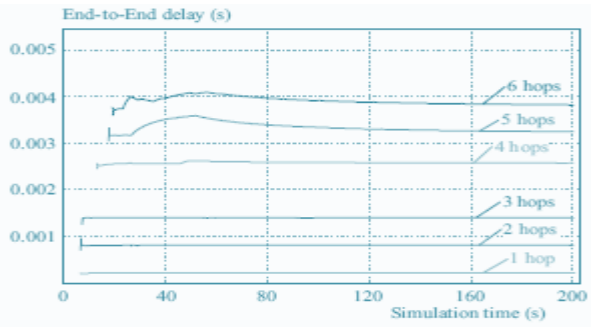

Figure 14. Architecture latency

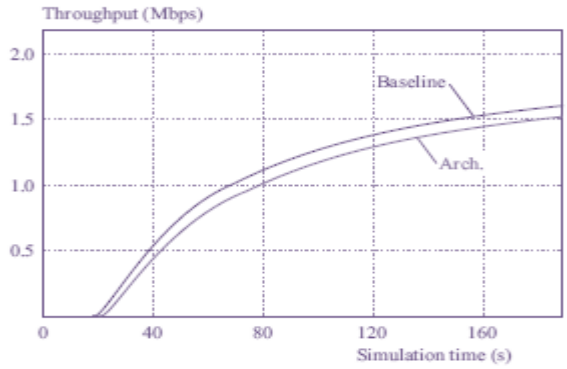

Figure 15. Architecture Throughput comparison

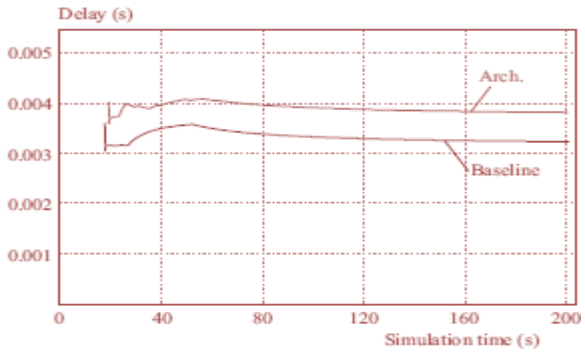

Figure 16. Delay comparison

V. CONCLUSION

We presented our own security architecture for MANETs in this paper. We evaluated the work involved and then identified our solution's inner workings. In a discrete simulation of events, we implemented it and presented the results. We found a 3 percent lower throughput compared to the existing solution and a 5 percent lower delay compared to the analyzed solution [3]. Comparing our solution's security, it is more comprehensive and advanced than any other solution examined. We supported secure routing protocol, PKI, Firewall definition and IPS for architecture. Nodes can have different privileges based on their level of trust and those privileges can be diminished or removed if there is a presumption of malicious behavior.

REFERENCES

[1] S. Akram, I. Zubair and M. Islam, ”Fully distributed dynamically configurable firewall to resist DOS attacks MANET”, rev. Networked Digital Technologies, 2009, NDT ’09.First International Conference, Ostrava, 2009.

[2] M. K.A. D.??? Alicherry, ”Distributed Policy Enforcement Architecture for MANETs”, Diploma work ???.

Copyright © 2019 Mélange Publications

[3] M. Alicherry, A. Keromytis and A. Stavrou, ”Evaluating a collaborative defense architecture for MANETs”, Rev. Internet Multimedia Services Architecture and Applications (IMSAA),2009, IEEE International Conference, Bangalore, 2009.

[4] R. Boppana and X. Su, ”On the Effectiveness of Monitoring for Intrusion Detection Mobile Ad Hoc Networks”, 2011.

[5] A. Boukerche, K. El-Khatib, L. Xu and L. Korba, ”SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks”, 2004.

[6] A. Chaudhary, V. Tiwari and A. Kumar, ”Design an anomaly based fuzzy intrusion detection system for packet dropping attack mobile ad hoc networks”, Gurgaon, 2014.

[7] D. Ismail and M. Jaafar, ”Mobile ad hoc network overview”, Melaka, 2007.

[8] L. Jin, Z. Zhang, D. Lai and H. Zhou, ”Implementing and Evaluating An Adaptive Secure Routing Protocol for Mobile Ad HocNetwork”, Pomana, CA, 2006.

[9] I. Khalil, S. Bataineh, L. Qubajah and A. Khreishah, ”Distributed secure routing protocol for Mobile Ad-Hoc Networks”, Amman, 2013.Unauthentifiziert | Heruntergeladen 17.10.19 05:05 UTC204 J. Filipek, L. Hudec: SECURITY ARCHITECTURE FOR THE MOBILE AD HOC NETWORKS

[10] N. Noureldien, ”A novel taxonomy of MANET attacks”, Marrakech, 2015.

[11] L. Rajeswari, R. Annie and A. Kannan, ”Enhanced intrusion detection techniques for mobile ad hoc networks”, Tamil Nadu,2007.

[12] S. Saha, R. Chaki and N. Chaki, ”A New Reactive Secure Routing Protocol for Mobile Ad-Hoc Networks”, Ostrava, 2008.

[13] B. Sun, L. Osborne, Y. Xiao and S. Guizani, ”Intrusion detection techniques mobile ad hoc and wireless sensor networks”,.

[14] S. Uyyala and D. Naik, ”Anomaly based intrusion detection of packet dropping attacks mobile ad-hoc networks”, Kanyakumari, 2014

[15] B. Vaidya, D. Makrakis and H. Mouftah, ”Provisioning secure on-demand routing protocol mobile ad hoc network”, Kathmandu, 2011.

[16] P. Vilhan and L. Hudec, ”Building Public Key Infrastructure for MANET with Help of BATMAN Advanced”, Rev. Modelling Symposium (EMS), 2013 European, Manchester, 2013.

[17] N. V. Vinh, H. Jun and M.-K. Kim, ”A Self-secure Routing Protocol for Large Mobile Ad hoc Networks”, Singapore, 2007.

[18] H. Zhao and S. Bellovin, ”High Performance Firewalls MANETs”, Rev. Mobile Ad-hoc and Sensor Networks (MSN), 2010Sixth International Conference, Hangzhou, 2010.

[19] L. Zhitang and S. Shudong, ”A Secure Routing Protocol for Mobile Ad hoc Networks”, Melbourne, Qld., 2007.

[20] D. Watkins and C. Scott, ”Methodology for evaluating the effectiveness of intrusion detection tactical mobile ad-hoc networks”,2004.

[21] J. Filipek and L.Hudec ”Distributed firewall using PKI mobile Ad Hoc networks”, Proceedings of the 16-th International Conference on Computer Systems and Technologies, CompSysTech’15.

Copyright © 2019 Mélange Publications