[Pradeep et. al., Vol.6 (Iss.5): May 2018]
(Received: May 04, 2018 - Accepted: May 29, 2018)
ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.29121/granthaalayah.v6.i5.2018.1464

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

A SURVEY ON AUTHENTICATION TECHNIQUES FOR WIRELESS MEDIUM

Pradeep M B [*1], Manjunath C R [2]
[*1] Department of CSE, SET, Jain University, Bangalore, Karnataka, India
[2] Associate Professor, Department of CSE, SET, Jain University, Bangalore, Karnataka, India

Abstract

The wireless communication technology gaining importance in extreme conditions in a very effective way due to its benefits. Compared to wired networks, wireless networks have many benefits in terms of flexibility, cost, and mobility. Wireless networks can be easily hacked by the outsiders if there is no proper security. Because of its increasing popularity, wireless networks need proper security measures in addition to the normal protections such as firewalls, virus detectors, etc. Providing the required additional security to the wireless networks is a challenging task. Security can be maintained by providing data authenticity, integrity confidentiality, and authorization. A survey on the security of wireless networks is put forward that discusses various techniques which help in protecting the network and a cryptic secure scheme has been proposed which helps to enhance the security standards in the wireless medium.

Keywords: Cryptic Scheme; Authentication; Encryption; QR Code; Trust Based Routing; Secure Communication.

Cite This Article: Pradeep M B, and Manjunath C R. (2018). "A SURVEY ON AUTHENTICATION TECHNIQUES FOR WIRELESS MEDIUM." *International Journal of Research - Granthaalayah*, 6(5), 369-376. 10.29121/granthaalayah.v6.i5.2018.1464.

1. Introduction

Wireless networks are the flexible data communication systems that use wireless media such as radio frequency technology to communicate with computers and other network devices over the air. Sometimes these networks are also called as WLAN or WIFI. Compared to wired networks, Wireless network offers some discrete advantages such as mobility, exclusion of wires, convenience, productivity, easy setup etc. Also, wired networks fail to provide flexibility and scalability.

Wireless networking has overcome some of the challenges of the wired network and also provides ease of deployment. Disadvantages of wireless technology include additional security and the interruptions in the radio signals (due to bad weather, other wireless devices or obstructions like a wall). Data that resides in the wireless networks can be easily hacked by the outsiders if there is

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1284538

no proper security measures are in place. Security in wireless networks determines the ability of the network to manage, protect and distribute sensitive information. With the help of additional security measures such as authentication, trust-based routing, and other schemes; we can have protected data communication. Authentication of nodes in a wireless network is very important due to its openness to various security threats. The architecture of simple wireless networks is shown in fig 1.

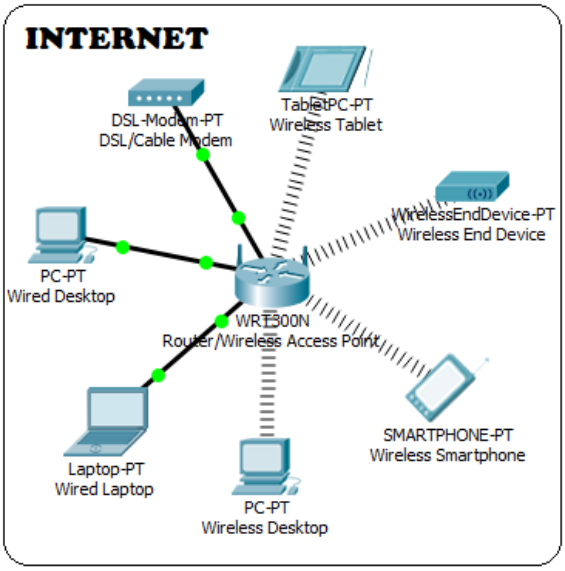

Figure 1: Architecture of Wireless Network

2. Related Work

2.1. Security Necessities in A Wireless Environment

In any wireless medium, data should be exchanged only between genuine users, due to the broadcasting character of the wireless networks the data is exposed to many threats. so it is very important to protect the network against attacks such as DOS attack, eavesdropping, etc. In general, wireless networks should fulfill security requirements such as authenticity, authorization, confidentiality, and non-repudiation to have secure communication.

1) Authenticity: It helps to confirm the genuine character of a node existing in a network to distinguish between the certified users from illegal users. In wireless network, when two nodes are communicating with each other, it is necessary for the node to achieve verification before setting up a link for data communication. Generally, network nodes have unique MAC address along with wireless network interface that can be used for the purpose of authentication.
2) Authorization: It is a process in which sever determines whether the client has the permission to access the data. Generally, authorization is combined with authentication so that it will be easy to grant the access to the genuine users. Sometimes, passwords can be used for data validation and in some other cases such as web pages on the internet do not require any authorization or the authentication. Additionally, authorization makes sure that only certified nodes are involved in a specific action.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
(Received: May 04, 2018 - Accepted: May 29, 2018) DOI: 10.5281/zenodo.1284538

3) Confidentiality: It is the process of limiting the data access only to the genuine users while preventing data access to the illegal users. Data confidentiality can be achieved with the help of encryption methods like hashing, symmetric key cryptography, and asymmetric encryption. In wireless communication, the eavesdropping attack can be prevented with the help of confidentiality which provides proper data privacy. Also in the wireless environment some of the information such as location details, route updates should be kept secret which can be done with the help of confidentiality.
4) Non-repudiation: It is the process of linking the users to perform some actions in such a way that they cannot reject. For example, if a user wants to add a non-repudiation feature to a document, he can attach a digital signature to the whole document using the private keys making sure that his partner doing the same. Now the users have no power to deny that they both approved the document, in the form that it appears.

2.2. Security Issues in Wireless Networks

The wireless networks are very vulnerable to attackers due to its openness feature. Summarization of wireless security requirements presented in [2] (Zou, 2016). It also studies some of the issues in wireless networks along with some techniques for improving security standards in a wireless environment. Some of the major attacks [12] (Sabina Barakovic, 2016) include Denial of service, packet sniffing and may be categorized based on security requirements which are major threats to the network. In wireless networks, many research papers focus on Authentication techniques. Some of the attacks are briefed below.

1) Traffic Jamming: The invader uses too much bandwidth to overcome the genuine by overflowing the information. These attacks can be classified as
   - DoS (Denial of Service) attacks: In wireless networks, a Dos attack happens when an attacker continuously attacks a wireless access point with different protocols which are considered to use the system information.
   - Spam attacks: The invader initiates the spam attacks by overflowing the spam data above the wireless environment.
2) Eavesdropping and Interception: The enemy node can eavesdrop or interrupt the genuine traffic with the help of legal user's wireless channel, thus gaining the access to the user's data. Some of the attacks include
   - Man in the middle attack: Here the data communication between two entities is observed and controlled by an unauthorized user.
   - Traffic Eavesdropping: Here the intruder uses the network sniffer to eavesdrop the traffic in a wireless network environment.
   - Network injection: This attack targets wireless access points which are exposed to non-filtered network traffic, such as network management messages or routing protocol messages.
   - Session Hijacking: Here invader takeaway the genuine authentic session ID of a particular conversation and controls the whole session.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
(Received: May 04, 2018 - Accepted: May 29, 2018) DOI: 10.5281/zenodo.1284538

3. Literature Survey

Because of the increasing popularity of wireless networks, we need additional levels of security. That is, along with normal password protection, firewalls, and virus detectors, it is better to have special security to address the specific issues associated with wireless communication. With the help of encryption techniques, proper authentication scheme along with authorization we can increase the security level of the network. Many techniques have been proposed for authentication and major ones are discussed here.

A review of wireless network threats that includes attacks related to access point, authenticity, confidentiality, and integrity, along with techniques that defend these attacks have been presented in [1] (Akhil Gupta, 2015).The attacks in the wireless environment are categorized based on the security requirements such as authenticity, confidentiality, integrity, and availability. The paper [2] (Zou, 2016) presents the summarization of Wireless Security Requirements along with some of the major threats in wireless technology and also it inspects capable defense method for improving the security standards in the wireless environment. In wireless networks, many research papers focus on Authentication techniques. For achieving secure communication in wireless networks authentication plays a very important role. To protect the network against the malicious activities SecRoute [3] (Hatzivasilis, 2017) proposes an end to end secure communication where authentication is based on TESLA [4] (Perrig,2005). The ultra-lightweight cryptographic library (ULCL) is used in order to implement TESLA, which provides node authenticity and message integrity. Here the authorization is provided by the policy based access control framework. A trust-based scheme TRAS [5] (Jawhar, 2016) protects the network and Trust of exposed routes among the source node and destination node is a major factor in order to achieve improved security in wireless communication. Authorization is an important component to achieve secured communication and here it is imposed by a policy-based access control framework [6] (Rantos, 2015). SecRoute [3] (Hatzivasilis, 2017) improves the network's security, with a good performance overhead for the end devices, also it includes trusted execution elements [7] (Shepherd, 2016), to protect against malicious activity. RFSN[11] (Srivastava, 2004) develops a community of trust for the nodes and makes it clear that only cryptography is not enough for proper security so It maintains proper trust ratings of the neighbors and is resilient to different attacks if Watchdog mechanism is properly.

The secure resilient based routing (SR3)[8] (Altisen, 2013) which is the combination of reinforced random walk algorithm with reputation. Here in the random walk algorithm, the node count is higher than other methods. The communication is considered as successful when a genuine acknowledgment is received, and then the reputation of the route nodes is increased. Here the Lightweight cryptography is incorporated for the purpose of data confidentiality, data integrity, and data authenticity. Another key establishment protocol [9] (Zhimeng, 2016) whose security mechanism totally depends on the computational Diffie Hellman problem. Here the nodes can establish safe communication with the help of other adjacent nodes over the node authentication and key exchange protocol in the adversarial model, which can protect key compromise impersonation attack. Another research paper [10] (Tang, 2008) describes an efficient authentication scheme, which is suitable for low power mobile devices. For generating a delegation code for mobile station authentication, it uses an elliptic-curve cryptographic system and also it can successfully defend all the known attacks including Dos attacks. A four-way handshake

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
(Received: May 04, 2018 - Accepted: May 29, 2018) DOI: 10.5281/zenodo.1284538

mechanism along with proper authentication scheme for key agreement [14] (JAEWON NOH, 2018) along with the ECC based public key cryptography defends the major security threats like eavesdropping. In order to increase the security, [13] (Mrs.A.S. Bhave, 2014) suggests a hybrid encryption scheme which is a combination of two algorithms AES and ECC. The AES has been precisely recommended as the most appropriate method for the wireless environment.

4. The Cryptic Scheme

The Cryptic scheme is a combination of three major components where Cryptic services provide authentication and data confidentiality, Trust-based routing defends against the routing attacks and policy-based access control framework provides authorization functionality.

Cryptographic Services

A Cryptographic Service provides authenticity, message integrity, and confidentiality. Cryptic scheme achieves data privacy by scrambling the data packets; for this, modified AES algorithm of key size 256 is used. Symmetric-key cryptography is used for data encryption.

AES Algorithm: Advanced encryption standard algorithm is a symmetrical key encryption system widely used to encode majority of data. It functions on a 4x4 column-major order matrix of bytes, called the state. The process mainly comprises repetitive series of certain permutations and combinations to change a simple text into complex data. We have achieved around 10 rounds to convert simple text into ciphertext.

Encrypting the Message: Most of the networks in modern communication accept symmetric key cryptography. The key management in symmetric key cryptography is very simple. The only single key can be used for the purpose of encryption and decryption. Here the key should be kept secured and the key should be protected from outsiders other than the user. To deal with this problem we have proposed a new method of generating a code from the entered password, which will act as a key. In this method, the key generated from the password will act as the first level of security of the encrypted message.

After the use of a symmetric key for the first level of encryption, (i) The encrypted message is then treated as a large string and the reverse of the string is generated. (ii) The reverse encrypted string then extracted bitwise and XOR operation is performed with ‘1’ (one) to those bits. This will generate another new encrypted message. (iii) This encrypted message is extracted bitwise and invert operation is applied to every 4th bit (Ex: 4^{th} bit, 8th bit, a 12^{th} bit...) of the message. Again XOR operation is performed with 1 to the resultant bits. This will generate another new encrypted message. (iv) Then that encrypted message is converted into QR Code as shown in figure 2.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1284538

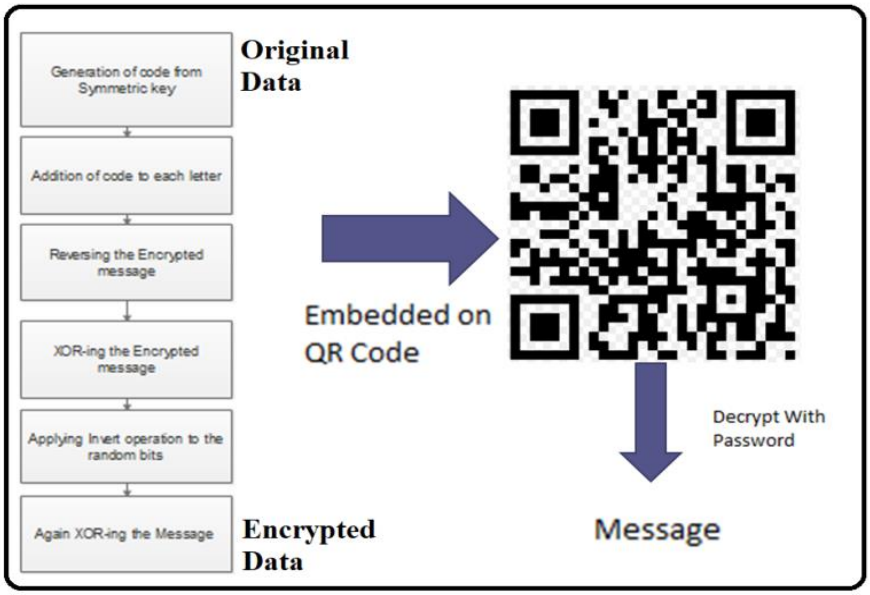

Figure 2: Encryption Process

QR Codes are very good at securing the data, so we can use it to hide the scrambled data in the QR code. (v)And now to decrypt the message, the first one has to know the key (password) or else the encrypted message will be shown and won't get the real message. After the key is entered to reveal the encrypted message the code will be created and the encryption system will be reversely handled to get back the original data.

Trust-Based Routing

Trust-based routing protocols are protocols that only accepts nodes with a trust above a certain minimum acceptable trust (MAT) in their routing table and use them for forwarding control/data packets so that each node to be part of the routing table, it should have a trust above a certain MAT. A trust-based routing protocol TRAS [5], is being adopted. Trust of discovered paths between the source and destination nodes is an important component towards achieving enhanced security in communication. The trust factor is increased when nodes participate successfully during the data transmission process by using an acknowledgment mechanism.

Policy-Based Access Control

Authorization is an important aspect of the network security. After protecting the routing mechanism and securing the correct data transmission, we should provide proper authorization functionality. In order to comfort the operational management of the system, it is better to adopt a policy based authorization on embedded devices. As the nodes start receiving the requests, it should be capable to make right decisions. A policy-based access control (PBAC)[6] framework has the ability to achieve direct access requests to the resources of an embedded device. PBAC framework is based on a predefined set of rules and policies. This framework consists of several components which can run on any node by providing the access to the resources and services. PBAC allows fine-tuned, policy-based access to resources from remote places.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
(Received: May 04, 2018 - Accepted: May 29, 2018) DOI: 10.5281/zenodo.1284538

Securing the wireless networks is a challenging task. Threats such as eavesdropping altering or inserting messages and disruptions are very much dangerous to the network. With the help of signal hiding techniques and encryption can provide defense against eavesdropping. The standard techniques to protect the network are by using some of the authentication protocols along with encryption. The major challenge in wireless networks is to prevent unauthorized attacks. Some of the authentication techniques provide a strong defense against attacks. Using symmetric key encryption makes the network secured which requires less cost and more protected against unauthorized access.

5. Conclusion

Wireless networks have applications in various fields and the gathered information is very sensitive. So it is necessary to protect the data with the help of proper security measures. In order to increase the security standards, we need have mechanisms that concentrate on data integrity, confidentiality, and authenticity. The paper provides security requirements and some of the issues related to security, besides some of the authentication techniques are briefed in this paper. The proposed scheme is a hybrid approach which is a combination of three main components where cryptic scheme provides data confidentiality and data integrity. Trust-based scheme protects the network against routing attacks. And Policy-based access Control framework helps to grant the authorization.

Many authentication techniques revolve only around security whereas other techniques concentrate on the challenges in the wireless networks. Since Authentication provides a good defense against the node tampering and also it requires sharing of keys. Therefore it is very important for secure communication. Also, an effective implicit authentication technique can minimize the computation cost and eliminates the need for a shared key. Furthermore, for secure communication, it is very important to have trust-based routing to protect the network from unauthorized nodes and also we can use better authorization scheme along with authentication techniques. With the help of literature, we can conclude that a hybrid approach which provides a unique authentication technique, authorization based on policies along with a trust-based scheme can provide the high-level security for wireless medium.

References

[1] Akhil Gupta, R. K. (2015). Security Threats of Wireless Networks: A Survey. *International Conference on Computing, Communication, and Automation*, 389-395.
[2] Altisen, K. D. (2013). SR3: Secure resilient reputation-based routing. *Distributed Computing in Sensor Systems (DCOSS)*, 258-265.
[3] Hatzivasilis, G. P. (2017). SecRoute: End-to-end secure communications for wireless ad-hoc networks. *Computers and Communications (ISCC), 2017 IEEE Symposium on. IEEE*, 558-563.
[4] Jawhar, I. M. (2016). TRAS: A Trust-Based Routing Protocol for Ad Hoc and Sensor Networks. *In Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on IEEE*, 382-387.
[5] Perrig, A. S. (2005). The TESLA broadcast authentication protocol. *Rsa Cryptobytes*, 1-13.
[6] Rantos, K. F. (2015). Policy-Controlled Authenticated Access to LLN-Connected Healthcare Resources. *IEEE Systems Journal*, 92 - 102.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1284538

[7] Shepherd, C. G. (2016). Secure and trusted execution: Past, present, and future-a critical review in the context of the internet of things and cyber-physical systems. *In Trustcom/BigDataSE/I SPA, 2016 IEEE*, 168-177.

[8] Srivastava, S. G. (2004). Reputation-based framework for high integrity sensor networks. *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 66-77.

[9] Tang, C. a. (2008). An efficient mobile authentication scheme for wireless networks. *IEEE Transactions on Wireless Communications*, 1408-1416.

[10] Zhimeng, L. a. (2016). Provable Secure Node Authentication Protocol for Wireless Sensor Networks. *Web Information Systems and Applications Conference*, 221-224.

[11] Zou, Y. Z. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE, 104(9)*, 1727-1765.

[12] Sabina Barakovic, E. K. (2016). Security Issues in Wireless Networks: An Overview. *2016 XI International Symposium on Telecommunications (BIHTEL)*, 1-6.

[13] Mrs.A.S. Bhave, M. (2014). Secure Communication in Wireless Sensor Network using Symmetric and Asymmetric hybrid Encryption Scheme. *IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.*, 382-385.

[14] JAEWON NOH, J. K. (2018). Secure Authentication and Four-way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks. *IEEE Access (2018)* , 16539 - 16548.

*Corresponding author.
E-mail address: iampradeep26@ gmail.com