IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 9 (September. 2018), ||V (IV) || PP 11-15

A Survey on User Authentication Methodologies by Channel Information in Wireless Networks

D. Priyadarshini[1], Faseela.P.Ismail[2]
ASSISTANT PROFESSOR, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India [1]
M.Phil Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India [2]
Corresponding Author: D. Priyadarshini

Abstract: *Wireless sensor networks (WSNs) are appropriate in adaptable domains varies from very ordinary to those which require vital security concerns. The use of WSNs in the surrounding and the resource-awkward character of the component sensor nodes give mount to an open challenge to guarantee that only authorized admit to the information is accessible through the sensor nodes. A lot of researchers have made significant hard work to meet up this dispute by scheming protected and trustworthy user validation mechanisms. Every projected method, with its pros and cons is cryptanalyzed to determine its relevant power and limitations. User authentication is the vital initially in order to detect identity-based attacks and preventing subsequent malicious attacks. The fine-grained channel information exposed in Channel State Information (CSI) has the possibility to execute correct user validation. A CSI-based user validation schema can efficiently exert with both immobile and mobile users. Especially, immobile user validation comprises an Attack-resilient User Profile Builder and Profile Matching Authenticator. The Attack-resilient Profile Builder utilizes clustering analysis to cleverly establish whether the network environment is lacking the occurrence of the identity-based attack when erecting the summary for the legitimate user.*

Index Terms- *User authentication, Wireless sensor networks, Gateway node, Sensor nodes.*

Date of Submission: 09-09-2018 Date of acceptance: 27-09-2018

I. INTRODUCTION

Wireless security is the avoidance of illegal admittance or smash up to computers using wireless networks. The most widespread types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a prominently powerless security standard. The password it avails can frequently be broken in a few minutes with a basic laptop computer and broadly accessible software tools. WPA was a rapid substitute to enhance protection. WPA2 avails an encryption device that encrypts the system with a 256-bit key; the enlarged key length enhances security over WEP. Firms regularly implement security using a certificate-based system to validate the linking device, which follows the standard 802.1X. The speedy improvement of wireless technologies has ended wireless networks omnipresent and therefore network services can be admitted at anytime and anywhere. However, protecting wireless networks is tough due to the mutual nature of the wireless medium, as opponent can overhear upon or interrupt any wireless transmission. For example, an opponent can inactively observe wireless networks to acquire legal device identities and additional commencement to identity based attacks, which provide as a basis for initiation of a variety of vicious hits across multiple network layers. Certainly, such identity-based attacks are simple to initiate in WiFi networks, where the Access Points (APs) can be miss-used, which results in Denial of Service. Though offered cryptographic based authentication methodologies such as WiFi Protected Access and 802.11i) can guard data frames, an attacker can still miss-use the 802.11 management frames. Moreover, the gradually more forceful mobile surroundings formulate it as tough to employ cryptographic-based validation, due to its framework and key management upward. Contemporarily authentication based on non cryptographic techniques has been projected to balance and improve the offered cryptography based schemes. An opponent, located at a diverse locality from the genuine user, will acquire different cryptographic profiles.

The initiative to privately organize, learn, observe and control a un tuned surroundings has given increase to the appearance of Wireless Sensor Networks (WSNs). WSNs are illustrated by ubiquitous environment and simple use; also provide an enormous combination of applications. Application areas of WSNs include but are not restricted to habitation observance, physical condition surroundings monitor, military purposes, interior sensor networks, manufacturing and consumer purposes, and avoiding chemical, biological, or nuclear threats in an area. Therefore, functionalities like home/building protection monitoring, monitoring

healthiness through machines and emergency medical care, controlling real time travel, battleground scrutiny and actions, for farming practices (temperature, humidity), quantity of seismic activity, manufacturing in factories, wild life monitoring, temperature and humidity control in museums, supervising voltage rise and fall in electric power companies etc, can be accomplished casually by means of WSNs. WSNs are really boon in falling the cost of framework by manufacturing it probable to organize the sensor networks in areas which were previously examined as cost unaffordable. Thus the variety of functionalities has improved to the amount which was once afar the attention of running with permanent sensor networks. A wireless sensor network comprises of numerous dozens to thousands of tiny sensor nodes (*SN*s)/devices surrounded with wireless transmitters. These sensor nodes have some handling power, inadequate estimation capacities, and inadequate energy and storage space. Besides with these abundant tiny sensor nodes, WSNs also contains some effective master nodes called base stations or Gateway nodes (*GWN*s). Tiny sensor nodes with two sensing factors are used to intellect compression, warmth, wetness, luminosity, etc. from their environment and commune with the nearby nodes and with the external world using an ad-hoc network *via* wireless links. When a wireless sensor network is organized in an area, the tiny sensor nodes instantly systematize in order to set-up a wireless network of ad-hoc nature. The sensor node intellect its neighboring circumstances and surpasses its measurement to the *GWN* or to a major location *via* network. The *GWN* practices the unprocessed data and guides the sensor nodes. Now days, image data of the environment can also be send out *via* WSN. The data so gathered from sensor nodes are notified to identify an exacting state or action in order to react and proceed with suitable result.

Owing to electricity utilization and calculation capability, user's queries are normally directed by the *GWN* rather than by *SN*s. The *GWN* behaves as a combination among the internet and the WSN. On the other hand, there are several scenarios where the role of the *GWN* is impractical and the user needs to directly admit the sensor nodes to acquire the necessary information; Although the data gathered in regards to warmth, compression or wetness in a particular region may not necessitate protection, for purposes like battleground observation, patient supervising, the composed information is significant and expects confidentiality and privacy of the expensive data. The open environment of WSNs is a profitable target for many cruel approaches. As the information or admission is offered to users on demand, so user validation is another chief concern alongside with modifications to the source inhibited character of WSNs. From the security perception of WSNs, the most vital feature is to guarantee suitable shared authentication between users and *GWN*, between *GWN* and *SN*s and between users and *SN*s. Consequently, the extremely guarded WSN environment does not effortlessly support Public Key Infrastructure (PKI) based methodologies. While, key management alongside with validation is necessary to assure the secure application of WSNs. Due to this issue the traditional validation procedures are not an ordinary fit for WSNs. However, the basic protection and service features of validation protocols like conflicts to estimate attacks, replay attacks, impression attacks, etc, and condition for shared validation between entities (user, *GWN*, *SN*) freedom to select and modify password, session key creation, etc, are uniformly vital in WSNs. Therefore manipulative of a user authentication protocol which is not only easy and proficient but also gathers safety and utilizable necessities of resource limitation WSNs and so unauthorized access can be prohibited from the situation is certainly a tough job. In this paper a survey has been taken by comparing the methodologies which can be used to authenticate Wireless Sensor Networks.

II. RELATED WORKS

In paper [1], a light-weight authentication and key management protocol for sensor networks has been projected. It fairly avails symmetric cryptography as well as, in specifically, UN keyed and keyed-hash functions. Encryptions are condensed to the least as well, with an encryption of little bytes to be executed by the applicant node one time per validation effort. This scheme gathers entire necessities regularly defined for sensor networks. Particularly, it offers a great flexibility across node acquire as, the negotiation of a node acknowledge that no information regarding links that is not directly associated in. It endows node-to-node identity validation too, as nodes are capable to validate the identities of the nodes they are communing with and an opponent is not capable to copy the identity of a node except this has previously been detained. In addition, the method has been intended to be challenging to denial-of-service attacks, which is very hazardous networks. The execution may look after of both cases with a time-out: if an issued dispute has not been properly responded in a threshold time, a, the challenge is noticeable again as 'UNUSED' and occurs accessible again. This limitation can be energetically familiar if an in-progress attack is identified, diminishing its significance regarding to the attack's cruelty.

In paper [2], authors projected to access received signal strength (RSS) which is depend on spatial association, a physical assets connected with each wireless device that is tough to fake and independent on cryptography as the foundation for discovering spoofing attacks in wireless networks. Authors offered theoretical analysis of accessing the spatial correlation of RSS obtained from wireless nodes for harass discovery. The resultant was the test guide based on the cluster analysis of RSS readings. This methodology can detect the occurrence of attacks as well as establish the quantity of opponents, faking the same node identity, so

that localization of any number of attackers is possible and also can be eradicated. Termination of the number of opponents is mostly a tough issue. For this purpose "SILENCE" has been widen, a mechanism that utilizes the smallest distance testing in adding up to cluster analysis to attain enhanced accurateness of resolving the quantity of attackers than other methods. Moreover, when the training data is obtainable, the examination of using Support Vector Machines (SVM) depending on the methodology to additional enhancement of the correctness by determining the quantity of attackers exists in the system. To validate this method, the accomplishment of experiments on two test beds through both an 802.11network (WiFi) and an 802.15.4 (ZigBee) networks. It was established that the discovery mechanisms are extremely effectual in both identifying the occurrences of attacks with invention rates over 98% and determining the number of opponents, attaining over 90% hit rates and accuracy at the same time when using SILENCE and SVM-based mechanism. Further, based on the number of opponents determined by this methodology, the incorporated detection and localization system can concentrate any number of opponents even when attackers using diverse transmission power levels. The attainment of localizing opponents accomplishes alike results as those under usual conditions, thereby, offering strong confirmation of the effectiveness of the approach in identifying wireless spoofing attacks, formatting the number of attackers and localizing adversaries.

In paper [3], a nonparametric Bayesian method to recognize wireless devices by their transmitter features, so as to avoid the attacks such as Sybil attacks and masquerade attacks. The unlimited Gaussian Mixture Model was employed for modeling, and a collapsed Gibbs sampling method was erected for device identification. From the replication and experimental results, the projected method established a finer attainment in identifying these attacks as well as discovering malicious nodes.

Observing in-home behavior [4] includes applications such as security monitor and healthiness organization. On the other hand, offering exact action identification without committed wearable or in-building devices is quite tough. Authors utilized the popularity of WiFi framework and propose a scheme called E-eyes to execute device-free location-oriented activity detection by employing the fine-grained channel state information (CSI) accessible in the existing WiFi protocol (i.e., 802.11n). It has been found out that CSI can arrest the distinctive patterns of small-scale vanishing originated by dissimilar human behavior at a subcarrier level, which is inaccessible in the conventional received signal strength (RSS) haul out at the per packet level. The system benefits from the examination that many vital in-home activities happen in one or a little committed locations and that it is therefore regularly adequate to gather a tiny quantity of profiles for these activities in each of these locations. E-eyes relates with matching algorithms to evaluate the CSI measurements beside familiar profiles to discover the activity. Extensive experiments in two different-sized buildings reveal that E-eyes is effectual in distinction a number of daily activities, and that it can attain a detection rate as high as 92%.

In paper [5], authors intended the Reciprocal Channel Variation-based Identification (RCVI), a mechanism to discover method for mobile wireless networks. RCVI utilizes the reciprocity of the wireless fading channel and RSS differences obviously acquired by mobility. It has been estimated that RCVI through theoretical analysis reflect on measurement errors, and authorize its possibility by means of experiments with off-the-shelf 802.11 devices underneath diverse attacking patterns and indoor and outdoor mobile circumstances. Experimental consequences illustrate that RCVI can attain desirable achievement under the tested scenarios. RCVI permits the user to adjust the stricture to attain sturdy protection but initiates negligible overhead.

In paper [6], a summary of diverse non-cryptographic means of user authentication and device recognition in both fixed and mobile wireless networks using lower/physical layer possessions or information. The pros as well as cons of this method and their execution issues are considered. Though most of the present methods illustrate the utilities in static wireless networks, restricted efforts have measured mobile cases. To precede the present research, two RSS-based authentication methodologies have been applied in mobile networks. The holistic cross layer security method accessing numerous layer information shared with conventional cryptographic mechanisms are fascinated in rising up the wireless networks.

Authors in paper [7], intended an original shared challenge-response validation method named PHY-CRAM, which is easy, less difficulty, strong, and scalable. By eradicating any training and synchronization progression, the CSI is reserved as a private to attackers; meanwhile the communication of mutual keys is safe by CSI. With an inexperienced attacker, PHY-CRAM attains approximately great achievement in thick multipath surroundings. When there remains a smart attacker, PHY-CRAM still works fine under most channel circumstances. Moreover, PHY-CRAM is sampled by FPGA and discrete RF components. Based on this prototype, the real world tests have been conducted to authenticate PHY-CRAM's attainment, and eradicated channel modeling error. This resultant proves that the reciprocal property of wireless channel is finely preserved when handing out interruption of the challenge-response signals and is very reliable.

In paper [8], authors studied on employing channel state information (CSI) to achieve sensible user validation in wireless networks. The fine-grained channel information exposed in CSI has the possibility to achieve correct user validation. A CSI-based user validation framework which comprises the Attack-resilient

User Profile Builder and Profile Matching Authenticator has been proposed. The Attack-resilient Profile Builder utilizes clustering analysis to cleverly resolve whether the network situation is without the occurrence of the identity-based attack when erecting up the profile for the genuine user. The Profile Matching Authenticator achieves packet level user validation grounded on Support Vector Machine (SVM). It has the capability to distinguish two users even when they possess the similar signal fingerprints.

In paper [9], authors depict that how wireless devices in closeness can pair separately by using their associated channel measurements from mobile wireless signals to outline a mutual crypto-key. The velocity with which users can strongly pair confides on their physical division, and on the speed of sequential differences in the selected channels. Coupling can be increased by observing numerous supplies concurrently, or by physically disturbing the valid devices together. It has been proved that using changes in phase, situated to extent differences establishes to be tough besides vigorous attacks. Finally, Proximate can simply be unlimited to permit beginning a familiar protected connection for more than two devices. It is trusted that a number of useful increments of Proximate can enhance its purposes and achievement smoothness added.

In paper [10], Management frame, the foundation for operating 802.11 networks usually, is tremendously weak to attacks. Spoofing detection lacking in supportive information is untrustworthy using present methods. Depending on off-the-shelf hardware, CSITE has been structured, a Wi-Fi management frame source validation system. It advances the distinctive features of CSI to ensure the authenticity of MFs, and the detection is adjusted to be extremely severe for False Positive (FP) errors. A method called CSI Resolution Enhancement (CRE) has been designed in order to successful delivery of MFs and also makes the MFs forward the detection with the use of ancestor frames has been designed. Widespread calculations are performed to authenticate the attainment of the system. These evaluations prove to be excellent validation capability and sturdy refusal besides spoofing attacks.

Table 1.0 Comparison Table

Pno	**Technique**	**Advantages**	**Disadvantages**
1	Key Establishment Scheme	Very light-weight, use has functions & symmetric encryptions, very efficient	Security has to be concerned
2	Spatial correlation	No need of additional cost, strongly effective	Little bit complicated, costly
3	Bayesian method	Prevent the attacks such as Sybil attacks and masquerade attacks	Time-consuming & frustrating
4	E-eyes	Very effective, accurate.	Activity recognition performance must be enhanced
5	Reciprocal Channel Variation-based Identification (RCVI)	Performs well, permits users to modify parameters	Fingerprint cannot be distinguished between different physical devices running the same software
6	Non-cryptographic authentication and identification schemes	Enhance existing cryptography-based mechanism, channel-based fingerprinting is most robust	Cannot achieve 100% detection, always trade-off between detection rate and false-alarm rate.
7	Physical layer Challenge-Response Authentication Mechanism (PHY-CRAM)	High successful authentication rate and low false acceptance rate	Weak in GSM-challenge protocols
8	Channel State Information (CSI) & Support Vector Machine (SVM)	Performs with accurateness and is intelligent, highly effective	Crucial for achieving reliable communication with high data rates in multi antenna systems
9	Proximate	Enhanced functionality and performance	Must use of non-binary quantization for improved extraction rates
10	CSITE architecture	Don't use extra burden to network traffic, fine authentication	Safety and efficiency are always contradictory

III. CONCLUSION

User authentication methods for WSN that were intended initially are unwrap to very clear threats like indoor attack, repeat attack, hijacker attack, etc. The vulnerability to indoor attack is because to the obedience of simple password during register phase. The accessibility to the hijacker attack is because to the stockpile of some user particular values in plaintext or in such a manner within some database that an attacker can acquire advantages of these values. Premature methodologies do not ease users to liberally modify their password at will. But enhanced versions not only occupied this failing but also included latest characteristics like shared validation and session key organization between one or more couple of entities involved. By keeping all the above concluding remarks of this paper, design and development of, SVM techniques work well with the time-cycle reduction and handles multi-variety data. Reliability and enhanced validations may be still improved.

REFERENCES

[1]. Delgado-Mohatar, Oscar, Amparo Fúster-Sabater, and José M. Sierra. "A light-weight authentication scheme for wireless sensor networks." *Ad Hoc Networks* 9.5 (2011): 727-735.
[2]. Yang, Jie, et al. "Detection and localization of multiple spoofing attackers in wireless networks." *IEEE Transactions on Parallel and Distributed systems* 24.1 (2013): 44-58.
[3]. Nguyen, Nam Tuan, et al. "Device fingerprinting to enhance wireless security using nonparametric Bayesian method." *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011.
[4]. Wang, Yan, et al. "E-eyes: device-free location-oriented activity identification using fine-grained wifi signatures." *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, 2014.
[5]. Zeng, Kai, et al. "Identity-based attack detection in mobile wireless networks." *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011.
[6]. Zeng, Kai, Kannan Govindan, and Prasant Mohapatra. "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]." *IEEE Wireless Communications* 17.5 (2010).
[7]. Shan, Dan, et al. "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks." *IEEE Journal on selected areas in communications* 31.9 (2013): 1817-1827.
[8]. Liu, Hongbo, et al. "Practical user authentication leveraging channel state information (CSI)." *Proceedings of the 9th ACM symposium on Information, computer and communications security*. ACM, 2014.
[9]. Mathur, Suhas, et al. "Proximate: proximity-based secure pairing using ambient wireless signals." *Proceedings of the 9th international conference on Mobile systems, applications, and services*. ACM, 2011.
[10]. Jiang, Zhiping, et al. "Rejecting the attack: Source authentication for wi-fi management frames using csi information." *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013.

D. Priyadarshini. "A Survey on User Authentication Methodologies by Channel Information in Wireless Networks. " IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 9, 2018, pp. 11-15.