Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Authentication of IoT-devices through Proximity Verification

M. Premalatha[1], D. Narender Singh[2]
[1]*Research Scholar, Dept. of Electronics & Communication Engineering, Anurag University, Hyderabad, India.*
[2]*Associate Professor, Dept. of Electronics & Communication Engineering, Anurag University, Hyderabad, India*
Email:[1] mpremalatha.432@gmail.com,
[2]dnarendarsingh@gmail.com

IoT-devices predominantly constitute embedded devices that lack an elaborate user interface, such as touchscreens or keyboards. Consequently, the conventional Pre-Shared Key (PSK) based authentication commonly employed for mobile devices faces challenges in its application. A case in point is our examination of home automation devices utilizing smartphones for PSK input, revealing vulnerabilities. The current process proves ineffective against active impersonation attacks and inadvertently exposes the Wi-Fi password to potential eavesdroppers. This security lapse renders IoT-devices susceptible to exploitation, posing a potential threat to critical infrastructures like home networks. Motivated by the real-world security vulnerability observed, this paper introduces a novel mechanism for IoT-device authentication known as Moving2Author. The primary objective is to fortify IoT-device security. In Moving2Author, users are required to hold a smartphone and execute one of two hand gestures—either moving towards and away or rotating—in proximity to IoT-device. The authentication process relies on the combination of two factors: (1) large Received Signal Strength (RSS) variation and (2) the alignment between the RSS trace and smartphone sensor trace. This combination enables Moving2Author to consistently and reliably detect proximity, facilitating the authentication of IoT-devices. Through our implementation on a Samsung Galaxy smartphone and a standard Wi-Fi adapter, we substantiate that Moving2Author effectively guards against potent active attacks. Specifically, the false-positive rate consistently remains below 0.5%, attesting to the robust security provided by Moving2Author.

Keywords: Pre-Shared Key (PSK), Received Signal Strength (RSS), IoT.

1. Introduction

This paper does experimental study conducted on a prominent home automation brand serves as a real-world illustration. The findings indicate that, through an attack on a single device, secrets can be gleaned, rendering them adequate for pilfering the home Wi-Fi password from all million devices in the system. The implications drawn from this tangible example underscore the imperative for a meticulously crafted authentication mechanism for IoT-devices. A comprehensive discussion and detailed experiments are expounded upon in Section II-A.

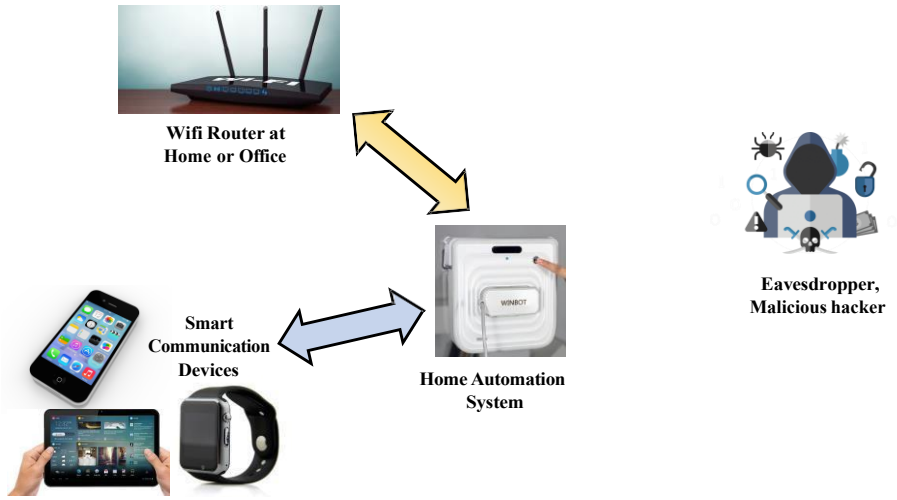

Figure.1. Using a home automation device as a case in point, we elucidate the authentication challenges associated with IoT-devices.

Within Figure.1, the illustration centers on a home automation scenario, offering insight into the authentication dynamics of IoT-devices. Wi-Fi router assumes the responsibility of authenticating home automation devices like a smart power switch.

Figure.2 Authentication of IoTdevices on proximity

Examining the scenario from the perspective of a Wi-Fi-router, IoT-device mirrors the characteristics of a mobile device, such as a smartphone or tablet. These devices commonly employ Pre-Shared Key (PSK) methods for authentication, wherein 802.11 standards integrate a Diffie-Hellman key exchange mechanism known as Simultaneous Authentication of Equals (SAE) for establishing mutual authentication between the router and the device. The incorporation of SAE, coupled with a limited number of authentication retries, presents a

viable solution against the depicted attacks in Figure.1. However, when viewed from the standpoint of IoT-device itself, a new set of challenges emerges. This is primarily attributed to the inherent limitations of IoT-devices, which typically lack avenues for PSK input, such as Wi-Fi passwords, due to their predominantly embedded nature. More specifically, the assumptions made here are twofold: first, that IoT-device lacks sophisticated user interfaces like screens or keyboards; second, it lacks auxiliary sensors such as cameras, accelerometers, gyroscopes, NFC, microphones, etc. Lastly, IoT-device under consideration is characterized by its limited mobility, exemplified by being fixed to a location (e.g., wall-mounted power switch).

For instance, methodologies requiring the simultaneous movement of both devices [4] or adherence to a predefined trajectory [5] are rendered impractical due to the absence of accelerometers/gyroscopes and the immobility characteristic of IoT-devices. A comprehensive exploration of the authentication predicaments and corresponding resolutions will be undertaken in Section II-B, offering a detailed exposition on why the unique nature of our problem necessitates a novel design approach. The papers mentioned in [11-17] introduces some more innovative techniques related to the problem of authentication of IoT-devices for industrial uses. The paper in [11] proposes a procedure of authenticating IoT-devices for a smart city infrastructure. The paper in [13] introduces a blockchain based method of identifying IoT-devices and authenticating them.

This document introduces a novel proximity-based authentication mechanism for smartphones to validate IoT-devices, termed as Moving2Author. As depicted in Figure.2, the prescribed methodology necessitates the user to grasp the smartphone and execute one of two hand gestures, randomly designated by the smartphone, in close proximity to IoT-device. Simultaneously, IoT-device continuously emits packets. The two gestures involve moving the smartphone towards and away from IoT-device and rotating the smartphone, inducing considerable (approximately 15dB) variations in RSS attributable to rapid fluctuations in attenuation and antenna polarization, respectively. Moving2Author amalgamates two primary components: (1) the detection of substantial RSS variations and (2) the correlation between the RSS trace and the smartphone's sensor trace. This amalgamation facilitates dependable proximity detection, wherein the first component effectively discriminates between devices in close proximity and those situated at a distance. The second component acts as a safeguard against potent active attackers with the capacity to arbitrarily adjust transmission power. This two-fold strategy enhances the robustness and security of the authentication process in Moving2Author.

The instantiation of Moving2Author is executed on the Samsung Galaxy smartphone in conjunction with a standard Wi-Fi adapter. A cohort of 5 users is enlisted to partake in prototype testing, encompassing experiments conducted within a test-bed featuring 12 distinct locations for IoT-devices. The empirical results derived from the evaluation illuminate two key findings: firstly, Moving2Author demonstrates a commendable level of reliability in effectively distinguishing between a sender situated in proximity and one positioned at a considerable distance. Secondly, Moving2Author exhibits robustness against potential active adversaries endowed with the capability to manipulate transmission power or possess access to the user's historical gesture traces. The observed false-positive rate in proximity detection consistently maintains a level below 0.5%.

Top works done here:

✓ Experimental investigations are undertaken to scrutinize the security aspects associated with the association of IoT-devices. Within this exploration, an undisclosed vulnerability is identified within a prominent home automation brand, indicating a heretofore unreported susceptibility. The revelations from this investigative inquiry serve as a catalyst for conceptualizing a dedicated authentication mechanism tailored explicitly for IoT-devices.

✓ The formulation, realization, and assessment of Moving2Author furnish a dependable mechanism for authenticating IoT-devices.

2. MOTIVATIONS AND RELEVANT LITERATURE

Within this section, a comprehensive examination unfolds, focusing on the experimental investigation into the association of IoT-devices. Throughout this scrutiny, an undisclosed security vulnerability surfaces within a widely adopted home automation brand, boasting millions of deployed devices. A meticulous dissection of this particular case transpires, fostering a compelling argument for the imperative development of a dedicated authentication mechanism tailored explicitly for IoT-devices. The explication delves into a detailed discourse on authentication challenges and their corresponding solutions, culminating in the impetus for the conception of a novel mechanism, introduced within the confines of this paper.

Despite the implementation of encryption in Wemo devices to safeguard Wi-Fi passwords, this measure proves insufficient in providing absolute protection. The acquired Wemo firmware is subjected to binary analysis, commencing with a preliminary string analysis that reveals the reliance on the prevalent Oss used in embedded applications, Open-WrT. Further analysis utilizes tools for analysing firmware, such as binwalk [15], to recover both the complete file system and individual program binaries. Subsequent manual identification of pertinent programs, primarily discerned by program names, precedes the utilization of disassembly tools like IDA [16] to convert program binaries into assembly codes. This disassembly process facilitates the extraction of cryptographic secrets embedded in the code. As anticipated, the encryption algorithm within the Wemo firmware employs OpenSSL libraries [17], employing a composite of the device ID and MAC address as key, initial vector, and salt in the encryption process.

The challenge of mobile device pairing, exemplified by interactions between two smartphones, shares similarities with the authentication concerns encountered in the context of IoT-devices. However, the distinguishing characteristics of IoT-devices, such as their limited mobility and absence of common sensors, set them apart. Consequently, authentication mechanisms relying on sensor-based approaches, including biometrics [10], accelerometers, gyroscopes [4], [5], and microphones [9], are not applicable to IoT-devices. Furthermore, explicit out-of-band channel methods, such as infrared [6], touch [7], or visible light [8], also find limited relevance in the context of IoT-device authentication.

Sensor network devices, categorized as embedded devices, share a certain affinity with IoT-devices. Nevertheless, a critical distinction arises from the fact that while IoT-devices may connect to an array of unknown access points, sensor network devices are typically tailored for specific applications, such as ocean or wildlife monitoring. These devices are often

manufactured in batches [20-21], allowing for the uniform distribution of identical Pre-Shared Keys (PSK) during the manufacturing process. This distinction underscores the unique challenges and considerations associated with the authentication of IoT-devices in comparison to sensor network devices.

Proximity-based mechanisms utilizing the radio interface, as documented in [4], [12]–[15], exhibit a close correlation with the solution proposed here. These mechanisms can be categorized into two types: passive and active. In passive solutions [12], [13], the proximity between two devices is discerned through a shared ambient radio environment. However, the efficacy of these solutions relies on a diverse range of ambient signals, presenting challenges in practice. Achieving sufficient variation in ambient signals often necessitates actions like shaking devices together or employing custom radios to sense additional signals such as FM and TV [23]. Such requirements are less favorable in the context of our problem. Additionally, passive solutions may mandate a relatively short distance between devices, typically a few centimeters on Wi-Fi frequencies.

Conversely, in active solutions, Castelluccia's approach [4] mandates coordinated shaking of two devices to confound eavesdroppers, rendering it unsuitable for our specific problem. Cai's [14] and Pierson's [15] solutions hinge on the utilization of multiple antennas to detect proximity through significant signal-strength disparities. While these approaches have inspired elements of our solution, notable distinctions exist. Firstly, instead of employing multiple antennas, our proposal leverages hand gestures to induce signal-strength differences, making it applicable to smartphones equipped with a single antenna. Secondly, our design not only relies on events of substantial signal-strength differences but also capitalizes on the correlation between device movement and signal-strength variations, thereby enhancing resilience against potent active attackers. Thirdly, our exploration extends beyond distance considerations to include device angle, exploiting signal-strength differences arising from antenna polarization in proximity scenarios.

3. DETECTION OF PROXIMITY ON THE BASIS OF RSS VARIATION

In the present work, a novel scheme centered around RSS is introduced, specifically tailored for proximity detection on devices equipped with a single antenna. The fundamental concept underpinning this approach is that the close proximity of two devices results in notable RSS variations induced by minimal device movements. The investigation focuses on two distinct types of movements, both of which lead to an approximate 15dB RSS variation: the act of moving towards and away from each other and rotational movement, as visually represented in Figure.2.

The substantial variations in Received Signal Strength (RSS) observed during movement towards and away from each other stem from the rapid fluctuations in channel attenuation that occur when two devices are in close proximity. While previously mentioned in [14], [15], the subsequent discussion is dedicated to elucidating the impact of antenna polarization, a phenomenon that induces significant RSS variations when two devices undergo relative rotation in proximity.

A. Polarization of Antenna

The fundamental concept behind Moving2Author lies in exploiting antenna polarization to induce profound fading events within the near field while remaining undetectable in the far field. This section aims to provide a concise overview of antenna polarization. At its core, the physics governing antenna polarization is grounded in radio wave polarization [25]. An exemplification of this principle is presented in Figure.3(a) using a dipole antenna, a prevalent antenna type in contemporary radio devices. The Figure.illustrates that the electric field consistently oscillates along the antenna direction, dictated by the constrained movement direction of electrons within the antenna structure. The phenomenon of antenna polarization engenders a unique characteristic wherein Received Signal Strength (RSS) undergoes variations contingent upon the angle formed between the transmitting (TX) antenna and the receiving (RX) antenna. The quantitative relationship governing this polarization-induced RSS change aligns with Malus' law [10].

$$F_{\varphi} = F_0 \cos^2\varphi + X_{\varphi} \qquad (1)$$

In the given context, the parameter φ represents the angle formed between the transmitting (TX) antenna and the receiving (RX) antenna. The variable F_{φ} denotes the antenna gain associated with the specific angle φ, and F_0 signifies the maximum antenna gain attainable when the TX and RX antennas are parallel and X_{φ} represents the fading coefficient.

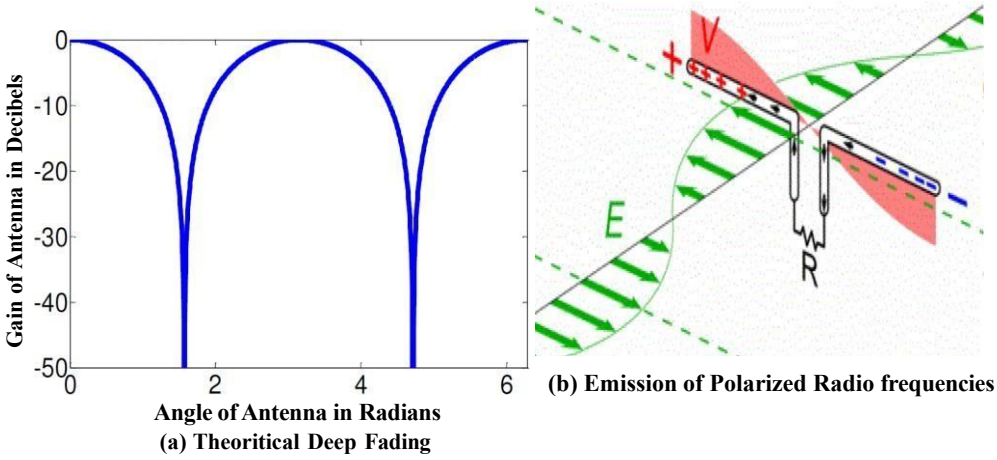

Figure.3 Gain of Antenna Variation with Antenna Angle

In practical applications, the validity of Equation 1 is confined to situations where two devices exist in close proximity.

Practical RSS-Variation

Figure.4 presents instances of Received Signal Strength (RSS) traces, illustrating scenarios where the sender is either in proximity or situated at a considerable distance, with the far-away sender positioned in an adjacent room to the receiver (smartphone). In the proximity scenario, the rapid fluctuations in attenuation result in an RSS variation exceeding 15dB.

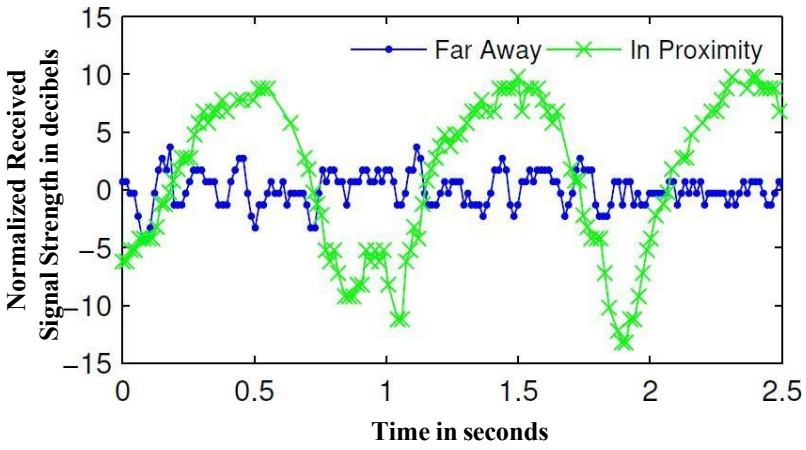

Figure.4 Analyzing RSS-Variation Due to Smartphone Movement in Sender Proximity vs. Far-Away Scenarios (Towards and Away)

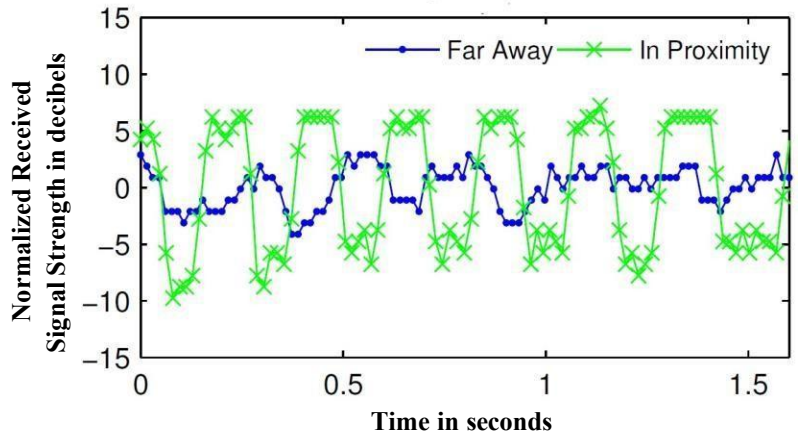

Figure.5 Analyzing RSS-Variation Due to Smartphone Movement in Sender Proximity vs. Far-Away Scenarios (Rotating)

4. MOVING2AUTHOR DESIGN

Within this section, the intricate intricacies of Moving2Author's design unfold, introducing an innovative mechanism tailored for the authentication of IoT-devices. While the design exhibits adaptability for integration with diverse radio technologies, the exposition primarily centers on its application within the Wi-Fi context.

In case of determining whether the communicating external IoT-device is a registered IoT-device or an eavesdropper we will be using the Support Vector Machine algorithm to study the patters of the RSS values in the Wifi router to determine whether it is an eavesdropper or a registered IoT-device. Equation 2 represents this algorithm. It is used for a framework of

learning that is semi-supervised.

$$g^* = \arg\min_{g \in J_I} \sum_j W(y_j, x_j, g) + \gamma_B \|g\|^2_B + \gamma_I \|g\|^2_I \text{ ---------- (2)}$$

In Equation (2) W() represents the function of loss, $\|g\|^2_\beta$ denotes the function norm in the Spcce of Reproducing Kernet Hilbert and $\|g\|^2_I$ denotes the function norm in low dimensions. $\gamma_B$and γ_I denotes the parameters for regularizing the weights.

A. Basic Scheme

The assumption is made that IoT device remains immobile during the pairing process. In pairing mode, IoT-device continually transmits encrypted packets, as elaborated in Section IV-G. Simultaneously, the user is tasked with holding the smartphone in close proximity (e.g., 20cm distance) to IoT-device and executing a brief gesture lasting, for instance, three seconds. The smartphone randomly selects one of two gestures, involving either approaching or moving away from IoT-device and performing a rotation, as depicted in Figure.2.

C. Trace Transformation - Moving Towards and Away

The user is instructed to displace the smartphone approximately 20cm, with the closest proximity to IoT-device also at 20cm. This deliberate movement results in an RSS-variation of approximately 15dB. This transformation involves initially converting the RSS-trace into a distance-trace, as outlined in [22, 24].

D. Trace Transformation - Rotating

The user is instructed to execute a 180° rotation of the smartphone, ensuring reliable capture of the RSS deep fading induced by antenna polarization, resulting in approximately 12dB RSS-variation. In our design, the gyroscope captures this rotation. As detailed in Section III and Figure.3, rotation induces deep fading in the RSS-trace due to antenna polarization. Our experimental results indicate that this design choice maintains a sufficiently low false-positive rate, as discussed in Section VI.

E. Time extent of Gestures of Utilizer

Here the initiation of the user gesture involves the act of pushing a (virtual) button on the smartphone. The error bar represents the deviation observed across 50 traces. Notably, when the traces extend beyond three seconds, the correlation result effectively distinguishes between the sender being in proximity and far away. As discussed in Section IV-D, the rotation inherently yields high correlation results for a sender that is far away. Consequently, in Moving2Author, we stipulate that the user must execute a gesture lasting minimum of 3 secs, and each trace from the sensor is trimmed below or equal to 3 seconds prior to undergoing match of traces.

F. Managing Inaccuracies in the collected

One challenge in the practical implementation of our scheme pertains to RSS Saturation, a phenomenon where the Received Signal Strength (RSS) reaches a maximum magnitude(for example -10.00 dBm over the platform designed by us) in cases if the transmitters coming very near (for example twenty centimeters). To address this, it becomes necessary for Internet-Of-Things based equipment transmitting at reduced quantities of power. From our empirical

observations, a reduction of 20dB in power of transmitting proves enough for prevention of saturating of the Received Signal Strength, a configuration easily achievable with commodity Wi-Fi chip sets. Another issue arises from the inconsistency in RSS readings associated by differing rates of information, especially in cases of differing rate of information transfers especially for differing preamble of packets. Consequently, we mandate that the devices connected to the Internet of Things employs minimum rates which is 6 Megabytes per second at the time of the authenticating process to ensure uniform and reliable RSS measurements.

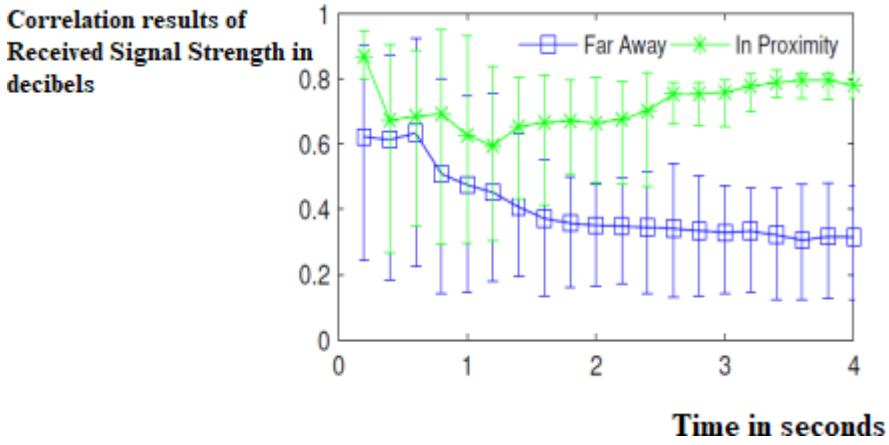

Figure.6 Results of correlation analysis of traces during rotating of the phone. The 3-sec gesticulation distinctly discriminates between the scenario where the sender is near-by and when the sending-party is at a long distance.

G. Encryption

In addition to the authentication mechanism elucidated earlier, a secure communicating pathways from devices connected to the Internet of Things and phones must be established to thwart potential secret listening. Approaches detailed in [26] offer methodologies for deriving a shared key based on wireless channel characteristics.

H. Moving2Author Scheme

The comprehensive scheme seamlessly amalgamates authenticating procedure of devices with generating of keys, unfolding in the subsequent steps: 1) Initialization commences when the user activates the modes of pairing via pressing of buttons in devices connected as internet of things for a duration of 3 secs. Simultaneously, the devices related to Internet of Things clear its pairing mode state following which they configures themselves like a point of access towards the phone for establishment of a connection. 2) The utilizer, in response, identifies the Network of Wifi variety for devices related to the Internet of Things through its SSIDs following which it proceeds to link up with phone and devices related to the Internet of Things. 3) Following the establishment of the links between devices related to Internet of Things with phones transmits a randomly generated key of public nature along with a sequence encryption based packs of similar sort using related keys of private type. 4) The smartphone, in the authentication phase, assesses the proximity of IoT-device by scrutinizing both the intensity of RSS-variation and aligning its sensor trace with the RSS trace. Refer to sections IV-C and

IV-D for detailed descriptions. 5) In the event of successful authentication, confirming the proximity of IoT-device, the smartphone validates keys of public nature through the decryption of transmitted packs following which their content are inspected. 6) Subsequent to the accurate decrypting of and verifying of the contents of the smartphone encryption is done via randomly generated keys of sessions that undergo sharing utilizing the authenticated public key, dispatching it towards devices related to IoT

I. Analysis of Security

In the current segment, a succinct scrutiny of Moving2Author's security is undertaken, encompassing diverse attack scenarios.

1) Eavesdropping: Given the resilience of public/private key cryptographic mechanisms, the potential for an adversary to glean information through packet sniffing remains negligible.

2) Impersonating IoT-device: In the context of smartphone-IoT pairing, a potential threat involves an attacker attempting to impersonate IoT-device by broadcasting identical SSID/MAC-address with heightened transmission power. The risk lies in the smartphone connecting to the attacker due to stronger signal strength. Moving2Author counters this by verification of if the equipment that is connected are placed near-by. This involves scrutinizing the attacker's compliance with schemes inside in section IV-H, where two cases are considered. If the attacker refrains from adjusting energy of transmitting, varying of Received signal strengths induced through locomotion of phones, will be minimal, mismatching the traces of the sensors and leading to authentication failure.

3) Denial-of-Service (DoS) attack: While Moving2Author doesn't explicitly guard against DoS attacks, the anticipated impact is considered manageable. Potential DoS tactics, like channel jamming, could disrupt communication, but the system's robustness is expected to handle such incidents. Rapid identification and removal of the attacker can be facilitated using localization tools.

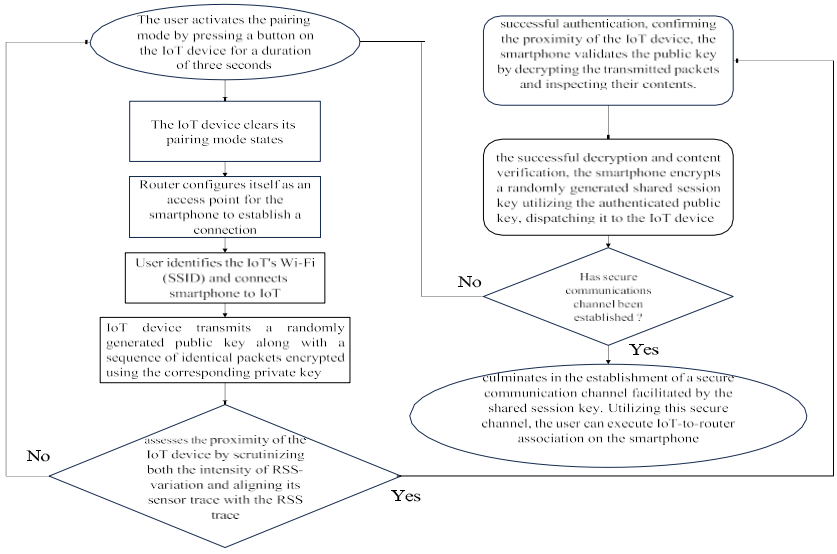

Figure.7 Flowchart representing Moving2Author protocol

5. EXPERIMENTS

A prototype of Moving2Author was developed on an Android smartphone using a standard Wi-Fi adapter. In case of this experiment we used a Wifi router with antenna length 3.1 cm and operating in the 2.4 Gigahertz frequency band. In case of the antenna in the smartphone we have considered for our experiment which is Samsung Galaxy S23 (which is enabled with 5G chipset) there are many antennas present – one of the is for cellular communications which is of size 1 to 2 mm in length, one of them is for Bluetooth based communications and it is of 0.5 to 1mm in length and another is for Wifi communications which is of 1 to 3 mm in length. In this case we will need to use only the Wifi antenna in the considered smartphone because we are talking about communicating with the Wifi router only. The experiment extended to Linux PCs equipped with Atheros and Intel Wi-Fi adapters, simulating the role of an IoT-device. The successful adaptation of Atheros and Intel Wi-Fi chipsets involved adjusting transmission power and fixing the data rate to align with Moving2Author requirements. To capture Received Signal Strength (RSS) on the smartphone, a custom Wi-Fi driver was installed, achieving monitor mode functionality. Presently, this driver is compatible with Samsung Galaxy 2 and 3 devices.

In the Moving2Author implementation, the recording of accelerometer and gyroscope outputs is initiated through a (virtual) button press. Timestamps were incorporated into both the RSS and sensor traces to facilitate subsequent trace-matching processes. Public/private key cryptography was implemented using the OpenSSL library.

The current Moving2Author implementation programs the Internet of Things devices (Linux PC) for transmission of packets at a rate of 1000Hz, with a 1ms interval between transmissions, ensuring a high-frequency sampling of RSS for authentication purposes.

EXPERIMENTAL RESULTS

This section outlines the evaluation of Moving2Author, emphasizing the reliability of proximity detection. Testbed, depicted in Figure.7, was established for the evaluation, covering 12 locations within and outside office-room (10m x 8m). The smartphone position was fixed at location-1. IoT-device moved to 12 positions, gestures were executed to gather RSS-traces. 5-utilizers evaluated, with 2-utilizers evaluations in IoT-device-areas and the remaining 3 users focusing on locations-1 and 12. Each test was repeated 10 times to generate statistically significant data. In total, six hundred traces from sensors along with traces from Received Signal Strengths were collected. RSS-variation threshold of 10dB and correlation threshold of 0.6 were fixed.

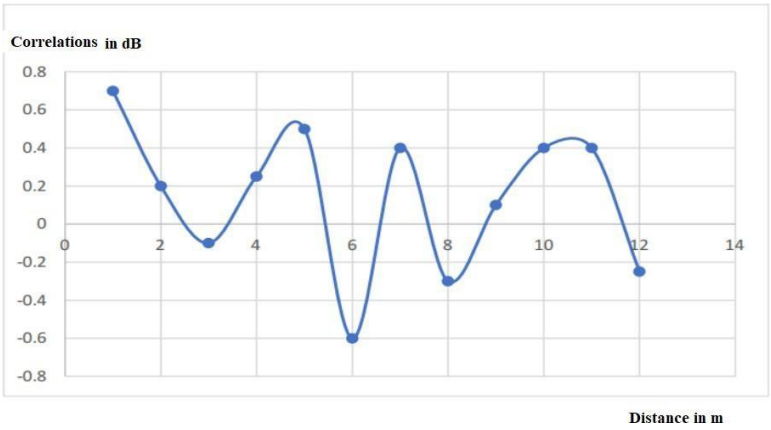

Figure.8 Variation of Correlation with Location Indices

A. Detection Rate In Proximity

Fig.8 provides statistical insights into all tests conducted at a specific location, encompassing data from various users. Notably, on 1st locations, both correlating along with RSS-varying metrics show higher outputs.

B. Far-away IoT-Device – based reliability measurements.

This scrutinizes false detection rate, evaluating instances where the smartphone inadvertently authenticates a far-away IoT-device. IoT-devices which are located at long distances, denoted as 2nd-location through Location-12, serve as the focal points for this evaluation, as illustrated in Figure.8.

Upon comparing the two distinct gestures, it becomes evident that the rotating gesture yields higher correlation results, aligning with the anticipated outcome elucidated in through Fig.8 and Fig.9. However, it is noteworthy that the rotating gesture is associated with relatively lower RSS-variation.

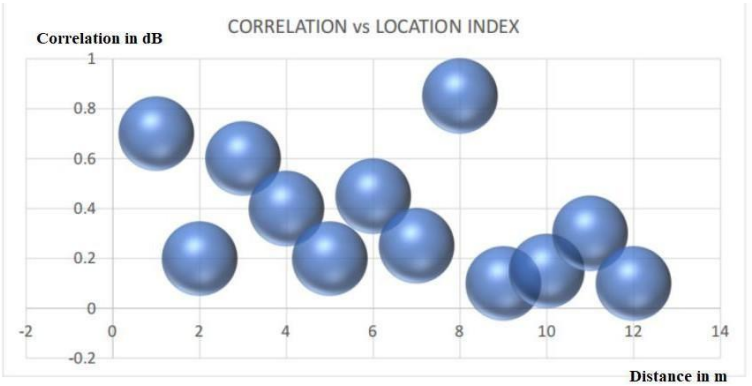

Figure.9 Change of Correlation values (y-axis) and RSS values with the change of Location Index (x-axis)

C. Reliability against Active Attacker

Firstly, a sine wave scenario is envisioned, assuming the attacker lacks knowledge about the user's gesture. This entails the exploration of various sine wave frequencies, with sixteen frequency-based equally distributed from 0.5GigaHertz to 4 GigaHertz tested. The attacking-party is assumed to transfer the Received Signal Strength waves incessantly. The CDF is in Fig. 9. Employing a threshold of correlating-data of 0.6 yields a false-positivity rates of 0.27%.

Second scenario involves an Received Signal Strength waves obtained from the gestures of other utilizers, possibly the attacking party itself. RSS trace-data got in each of the 5 utilizers on the first locations (in proximities) are collected, and correlations is computed across different users, considering various trace start times. The Cumulative Distribution Function of correlating data results in case of the current cases are illustrated in the top-right of Fig. 9, with a false-positivity rates of 0.31%.

Scenarios in the 3rd instances does exploration of history-based Received Signal Strength waveforms whose recording has been done from similar utilizers. Net trace-data of Received Signal Strengths obtained by similar utilizers on 1st Locations (in terms of proximities) are collected, and correlations are computed across differing trace-data from similar utilizers, considering various trace start times. The Cumulative Distribution Function of correlating data results in case of the current cases are presented in the bottom-left of Figure10, yielding a false-positive rate of 0.28%.

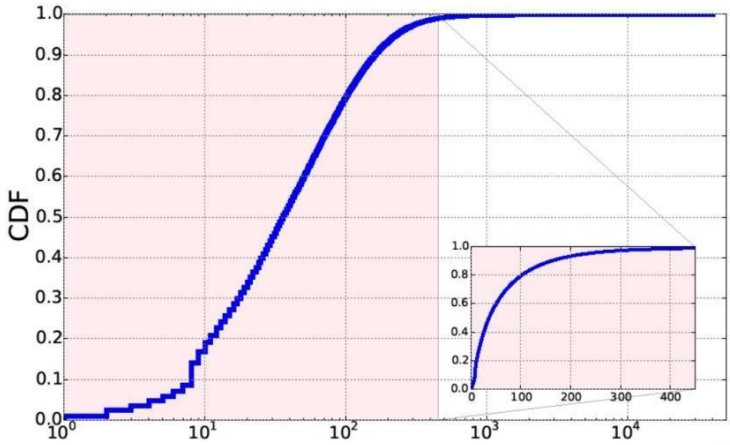

Figure.10 CDF depicting the correlating procedure (matching of traces) outcomes between the traces from sensors and the variations in Received Signal Strength (RSS) introduced by an attacker.

The results, depicted in the bottom-right of Figure.9, reveal an increased false-positive rate, albeit remaining small at 8.2%. Emphasizing the critical role of timing information in trace-matching, it serves as a deterrent even in the context of the most formidable (albeit non-realistic) attacker. However, it is essential to note that such an attack is implausible in real-world settings.

D. Comparison with existing wireless IoT-device authentication procedure [18]

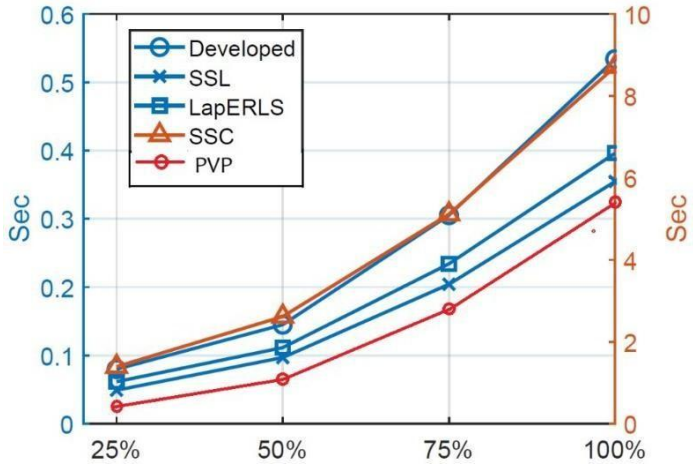

Figure.11. Comparing run-time for uploading of waveform-pattern in Wifi-router w.r.t [18]

In Figure.11 presentation of time to upload waveform in wifi-router for detection-authentication of device and compared it with other methodologies that have been proposed in Ref.[18]. From the simulation results that have been obtained it was found that the proposed PVP method or Proximity Verification Method (mentioned as PVP in Figure.12) takes lesser time in getting detected and uploaded in the wifi router.

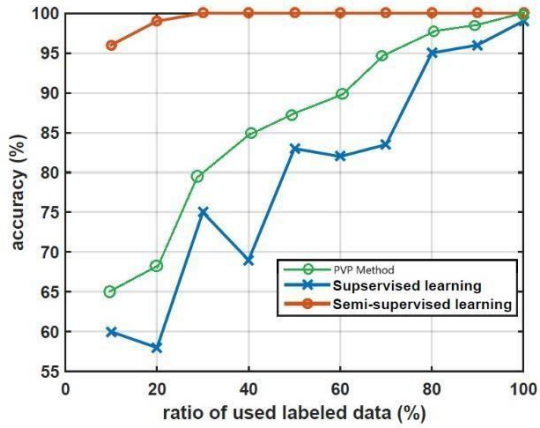

Figure.12. The outcomes of the analysed algorithms in terms of localization when the labeled training data percentage is altered: the execution time of the semi-supervised algorithms under comparison during pseudo-labelling in relation to the utilized training data

In Figure.13 we have presented level of accuracy that can be achieved by the use of the proposed PVP framework compared to the other algorithms which have been presented in [18]. Here we used our proposed scheme in similar manner to get the evaluation of accuracy of detection of the accurate waveform from the correct IoT-device. The proposed scheme is better than Supervised-learning scheme but low-accuracy than the semi-supervised learning scheme.

6. CONCLUSIONS

Derived from the real-world identification of security vulnerabilities in IoT systems, the authors introduce Move2Auth, an innovative proximity-related authentication implementation procedure tailored for IoT-devices. This mechanism operates by scrutinizing (1) substantial fluctuations in Received Signal Strength (RSS) and (2) the congruence between RSS-trace and smartphone sensor-trace during specific user gestures—namely, advancing or retreating the smartphone from IoT-device and rotating the smartphone. The implementation of Move2Auth on a Samsung smartphone substantiates its resilience against potent active adversaries.

References

1. "Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015," http://www.gartner.com/newsroom/id/3165317.
2. T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in Proceedings of the 14th ACM Workshop on Hot Topics in Networks. ACM, 2015, p. 5.
3. D. Harkins, "Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks," in Proceedings of the 2008 Second International Conference on Sensor Technologies and Applications, ser. SENSORCOMM '08, 2008, pp. 839–844.
4. R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," Mobile Computing, IEEE Transactions on, vol. 8, no. 6, pp. 792–806, 2009.
5. I. Ahmed, Y. Ye, S. Bhattacharya, N. Asokan, G. Jacucci, P. Nurmi, and S. Tarkoma, "Checksum gestures: continuous gestures as an out-of-band channel for secure pairing," in Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous
6. Computing. ACM, 2015, pp. 391–401.
7. D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks." in NDSS, 2002.
8. D. G. Park, J. K. Kim, J. B. Sung, J. H. Hwang, C. H. Hyung, and S. W. Kang, "Tap: touch-and-play," in Proceedings of the SIGCHI conference on Human Factors in computing systems.
9. N. Saxena, J.-E. Ekberg, K. Kostiainen, and N. Asokan, "Secure device pairing based on a visual channel," in Security and Privacy, 2006 IEEE Symposium on. IEEE, 2006, pp. 6–pp.
10. D. Schurmann and S. Sigg, "Secure communication based on ambient audio," Mobile Computing, IEEE Transactions on, vol. 12, no. 2.
11. E. Fernandes, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," in Proceedings of the 37th IEEE Symposium on Security and Privacy, May 2016.
12. R. Sharma, R. Rohit, and R. Arya, "A secure authentication technique for connecting different IoT-devices in the smart city infrastructure," Cluster Computing, vol. 25, no. 4, pp. 2333-2349, 2022.
13. L. Li, H. Qu, H. Wang, J. Wang, B. Wang, W. Wang, J. Xu, and Z. Wang, "A Blockchain-Based Product Traceability System with Off-Chain EPCIS and IoT-device Authentication," Sensors, vol. 22, no. 22, pp. 8680, 2022.
14. D. R. Bhuva and S. Kumar, "A novel continuous authentication method using biometrics for IoT-devices," Internet of Things, vol. 24, pp. 100927, 2023.
15. T. Ahsan, F. Z. Khan, Z. Iqbal, M. Ahmed, R. Alroobaea, A. M. Baqasah, I. Ali, and M. A. Raza, "IoT-devices, user authentication, and data management in a secure, validated manner through the blockchain system," Wireless Communications and Mobile Computing, vol. 2022,

pp. 1-13, 2022.
16. H. Goswami and H. Choudhury, "Remote Registration and group authentication of IoT-devices in 5G cellular network," Computers & Security, vol. 120, pp. 102806, 2022.
17. V. O. Nyangaresi, A. J. Rodrigues, and A. A. Al Rababah, "Secure Protocol for Resource-Constrained IoT-device Authentication," International Journal of Interdisciplinary Telecommunications and Networking (IJITN), vol. 14, no. 1, pp. 1-15, 2022.
18. A. Adeel, M. Ali, A. N. Khan, T. Khalid, F. Rehman, Y. Jararweh, and J. Shuja, "A multi-attack resilient lightweight IoT authentication scheme," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, pp. e3676, 2022.
19. J. Yoo and J. Park, "Indoor localization based on Wi-Fi received signal strength indicators: Feature extraction, mobile fingerprinting, and trajectory learning," *Applied Sciences*, vol. 9, no. 18, p. 3930, 2019.
20. Y. Liu, A. Liu, Y. Xia, B. Hu, J. Liu, Q. Wu, and P. Tiwari, "A blockchain-based cross-domain authentication management system for IoT-devices," *IEEE Transactions on Network Science and Engineering*, 2023.
21. Y. Ali, S. W. Shah, and W. A. Khan, *Security at the Internet of Things*, CRC Press, 2023.
22. M. H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods," *Journal of Big Data*, vol. 11, no. 1, pp. 1-39, 2024.
23. D. Marabissi, A. Abrardo, and L. Mucchi, "A new framework for Physical Layer Security in HetNets based on Radio Resource Allocation and Reinforcement Learning," *Mobile Networks and Applications*, pp. 1-9, 2023.
24. H. Farrukh, M. O. Ozmen, F. K. Ors, and Z. B. Celik, "One key to rule them all: Secure group pairing for heterogeneous IoT-devices," in *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 3026-3042, IEEE, 2023.
25. W. Xu, J. Zhang, S. Huang, C. Luo, and W. Li, "Key generation for Internet of Things: A contemporary survey," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1-37, 2021.
26. https://en.wikipedia.org/wiki/Polarization_(waves)
27. T. Lu, L. Chen, J. Zhang, C. Chen, and A. Hu, "Joint precoding and phase shift design in reconfigurable intelligent surfaces-assisted secret key generation," *IEEE Transactions on Information Forensics and Security*, 2023.
28. Singh, D. Narendhar, M. Hema, and M. Joseph Stalin. "IoT Based Healthcare Monitoring for Driver's Community." International Journal of Engineering Science and Computing (2017)
29. Narendar Singh.D, Pavitra.B, Nagaswetha.R, Anil Kumar G, Ashwini.G. (2022). An Intelligent Virtual Assistant using Raspberry Pi. Mathematical Statistician and Engineering Applications, 71(3), 1261–1270.
30. M. Premalatha and Dr. D Narendar Singh, "Increased Efficient Usage of Power in Cognitive Radio Networks Utilizing Hybridized Handover of Spectrum," 2024 5th International Conference for Emerging Technology (INCET), Belgaum, India, 2024