IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Detection Mechanism against the Attacks in MANET and Biometric Classification

P. Prabhusundhar[1*], B. Srinivasan[2], M. Ramalingam[3]

[1,2,3] Dept. of Computer Science, Gobi Arts & Science College (Autonomous), Gobichettipalayam, Tamilnadu, India

[*]*Corresponding Author: drprabhusundhar@gmail.com, Tel.: +91 9600877997*

Available online at: www.ijcseonline.org

Accepted: 19/May/2018, Published: 31/May/2018

***Abstract* -** Blackhole attack revealing, PCBHA (Prevention of a Co-operative Black Hole Attack) is a reviewed AODV routing protocol that is proposed in order to avert cooperative black holes. First, it runs each authorized user with a default fidelity level and after spreading a RREQ, a source node waits to accept resumed RREPs from the adjoining nodes and then chooses a near node of a greater fidelity level, which exceeds the threshold value, for passing the information packs. The target node will yield an ACK note after getting information packets, and the source node may add 1 to the fidelity level of the adjacent node, upon receiving of an ACK answer. If no ACK reaction is established, 1 is deducted from the fidelity level, which shows a potential black hole node on this route and information packets are released before reaching the end point node.

Keywords – Biometrics, Attacks, Secrecy, MANET

I. INTRODUCTION

Attacks in Manet: Sinkhole attack detection: Secure aware routing protocol detects and avoids the sinkhole attacks. In the SAR protocol, security measures are embedded in RREQ packet. When the particular node receives RREQ it verifies whether it is capable to provide the desired security features. If it provides the security features, then it is forwarded to the next hop otherwise the packet is dropped. SAR provides two security measures, trust hierarchy and security capabilities.

Wormhole attack detection: Packet leash is a mechanism for detecting and defending wormhole attacks. A leash is designed to restrict the packets maximum allowed transmission distance. This leash information is added to the packets. Two types of leashes are geographical leashes and temporal leashes. In a geographical leash, each node knows its position. Before sending a packet, it sends position and transmission time. On reception of the packets, receiver computes the distance to the sender and the time it took the packet to traverse the path. From this attack is detected. On the other hand, in a temporal leash, the sender appends the sending time to the packet and the receiving nodes computes the travelling distance of that packet.

Rushing attack detection: A set of generic mechanisms that together defend against the rushing attack: secure Neighbor Detection, secure route delegation and randomized ROUTE REQUEST forwarding. In previous on-demand protocols, node B considers node A to be a neighbor when B receives a broadcast message from A. Secure Neighbor Detection, which replaces standard Neighbor Detection, allows each neighbor to verify that the other is within a given maximum transmission range. Once a node A forwarding a ROUTE REQUEST determines that node B is a neighbor (that is, is within the allowable range), it signs a Route Delegation message, allowing node B to forward the ROUTE REQUEST. When node B determines that node A is within the allowable range, it signs an Accept Delegation message. Randomized selection of the ROUTE REQUEST message to forward, which replaces traditional duplicate suppression in on-demand route discovery, ensures that paths that forward REQUESTs with low latency are only slightly more likely to be selected than other paths.

Sybil attack detection: Trusted certification: In this detection mechanism, Centralized authority is set up for providing single identities for the nodes. Each entity in the network is bound to a single identity certificate. If centralized node fails, whole network will fail. Trusted Devices: Network card is bound to all of the entities in ad hoc network. But, attacker may sometimes install two or more network cards. Received Signal Strength: In this detection mode, whenever the node enters into the radio range and if it is in gray zone then it is called as a normal node otherwise if it is in white zone then it is called as a sybil node [Rajakumar.P et al., 2014].

Biometrics and Mobile Device: Biometric systems can be integrated with mobile devices such as cell phones in two ways: As a biometric collecting device or as a stand-alone system in order to protect unauthorized use of the mobile device such as cell phone. In the first case Mobile devices are used as collecting the biometric and then they are passing it via internet a remote location (e.g., server) where it is processed and matched. This proves the usefulness for

remote transactions when the identity of the user has to be proven. As an example, the user log in to the bank account through the mobile web browser or through banking software to make a transaction. The voice recording is done at the mobile device and then sends to the server to be processed and compared with the sample that was collected when the user enrolled in the system. Face, signature or key strokes are other biometric traits and today's mobile devices have the capabilities to collect and transfer them to remote location.

The other implementation of biometric system on mobile devices is the entire biometric authentication system resides on the mobile device and it serves the purpose of preventing unauthorized access to the mobile devices, functions and data. Today's implementations of biometric systems on mobile devices include face recognitions, voice recognitions, gait recognitions, signature recognitions and keystroke recognitions for unimodal or multimodal authentication [Pocovnicu.A, 2009] [Md. Saifur Rahim, 2010].

Rest of the paper is organized as follows, Section I contains the introduction of the attacks in MANET, Section II contains the classification of biometrics, Section III contain describes results and discussion about the detection mechanism against the attacks in MANET.

II. BIOMETRICS CLASSIFICATION

They involve two categories: Physiological Biometrics and Behavioral Biometrics.

A. Physiological Biometrics

In this category the recognition is based on physiological characteristics. Some examples are: Fingerprint, Hand Geometry, Iris Recognition, Retinal Scanning and Facial Recognition.

Fingerprint Recognition: Fingerprint is a unique feature to an individual. The lines that create fingerprint pattern are called ridges and the spaces between the ridges are called valleys or furrows. Through the pattern of these ridges and valleys, the unique fingerprint is matched for authentication and authorization.

Hand Geometry Recognition: This technology verifies a person's identity by the size and shape of the hand. The front part of the hand is used for hand geometry measurements. A set of features have been identified that could be used to represent a person's hand. These features include the finger thickness, length and width, the distances between finger joints and the hand's overall bone structure.

Iris Recognition: The iris of a human being can be used for biometric verification or identification through the process of iris recognition. It is not genetically determined (which means genetically identical eyes, e.g. the right and left eye of any given individual have unrelated iris patterns) and it is believed to be stable throughout life. Iris recognition technology is known for its extreme accuracy.

Retinal Scanning: Retinal scanning technology is used to measure the unique configuration of blood vessels located in the eye. The retinal image is difficult to capture and during enrollment the user must focus on a point while holding very still so the camera can capture properly. As the iris retinal recognition is generally considered to offer the best security because of the distinctiveness of the patterns and the quality of the capture devices.

Facial Recognition: The "passive" nature of face recognition makes it more suitable for wide range surveillance and security applications. In particular, an automated face recognition system is capable of capturing face images from a distance using video camera and the face recognition algorithms can process the data captured: detect, track and do the recognition. Face recognition focuses on recognizing the identity of a person from a database of known individuals.

B. Behavioral Biometrics

Behavioral biometrics is traits that is learned or acquired over time as differentiated from physiological characteristics. Some examples are: Voice Recognition, Signature Recognition and Keystroke Recognition.

Voice Recognition: Voice is a behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities and lips) that are used in the synthesis of the sound.

Signature Recognition: The way a person signs his name is known to be a characteristic of that individual. Signature requires contact with the writing instrument and physical effort of the user. Signature recognition systems, also called dynamic signature verification systems, measure both the distinguishing features of the signature and the distinguishing features of the signing process.

Keystroke Recognition: It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometric is not unique to every individual but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations in typical typing patterns. [Salah M. Rahal et al., 2006].

- Universality: Everyone should posses the trait to access the application.
- Uniqueness: The trait should be sufficiently different among individuals comprising the population.

- Permanence: The characteristic should be sufficiently invariant with respect to the matching criterion over a period of time.

There are seven factors defined by A. K. Jain et al., [1998] that determine the suitability of a physical or a behavioral trait to be used in a biometric application.

- Collectability: The characteristic should be measured quantitatively.
- Performance: The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
- Acceptability: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.
- Circumvention: This reflects how easily the system can be fooled using fraudulent methods.

Table 2. presents a brief comparison of the physiological and behavioral biometric techniques based on these seven factors described [A. Jain et al., 2004].

C. Unimodal Biometric System

Unimodal Biometric system depends on single biometric trait. Single biometric trait is used for person's identification or verification. This system is used for various applications. It is also used for the security purpose. Though the system has a wide range of application it can be affected by following drawbacks.

Noisy Data: Due to noisy data the matching is inaccurate that leads to false rejection.

Intra class variation: Intra class variation increases the false rejection rate. It is occurred due to the biometric data acquired is not same as the data used to create the template.

Table 1: Comparison of biometric technologies [A. Jain et al., 2004]

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	HIGH	LOW	MEDIUM	HIGH	LOW	HIGH	LOW
Finger print	MEDIUM	HIGH	HIGH	MEDIUM	HIGH	MEDIUM	HIGH
Hand geometry	MEDIUM	MEDIUM	MEDIUM	HIGH	MEDIUM	MEDIUM	MEDIUM
Keystrokes	LOW	LOW	LOW	MEDIUM	LOW	MEDIUM	MEDIUM
Hand veins	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH
Iris	HIGH	HIGH	HIGH	MEDIUM	HIGH	LOW	HIGH
Retinal scan	HIGH	HIGH	MEDIUM	LOW	HIGH	LOW	HIGH
Signature	LOW	LOW	LOW	HIGH	LOW	HIGH	LOW
Voice	MEDIUM	LOW	LOW	MEDIUM	LOW	HIGH	LOW
Facial thermograph	HIGH	HIGH	LOW	HIGH	MEDIUM	HIGH	HIGH
Odor	HIGH	HIGH	HIGH	LOW	LOW	MEDIUM	LOW
DNA	HIGH	HIGH	HIGH	LOW	HIGH	LOW	LOW
Gait	MEDIUM	LOW	LOW	HIGH	LOW	HIGH	MEDIUM
Ear Canal	MEDIUM	MEDIUM	LOW	MEDIUM	MEDIUM	HIGH	MEDIUM

Inter class similarities: Inter class similarities are due to the overlapping of feature space due to multiple individuals. It leads to increase the FAR (False Acceptance Rate).

Non universalities: Due to illness or disability some persons cannot provide required biometric.

Distinctiveness: Inter-user similarity refers to the overlap of the biometric samples from two different individuals in the feature space. Biometric trait is expected to vary significantly among individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discrimination power provided by the biometric trait.

Spoofing: An individual may use fake the biometric trait. It is easy for behavioral characteristics, such as when signature and voice are used as an identifier.

To overcome these drawbacks Multimodal Biometric system is used [Rupali L, Telgad et al., 2014].

A unimodal fingerprint verification and classification system is presented by [Prabhakar, et al., 1998]. The system is based on a feedback path for the feature-extraction stage, followed by a feature-refinement stage to improve the matching performance. This improvement is illustrated in the contest of a minutiae-based fingerprint verification system. The Gabor filter is applied to the input image to improve its quality. Ratha et al., [2000] proposed a unimodal distortion-tolerant fingerprint authentication technique based on graph representation. Using the fingerprint minutiae features, a weighted graph of minutiae is constructed for both the query fingerprint and the reference fingerprint.

Concerning iris recognition systems in feature [Vincenzo Conti et al., 2010], the Gabor filter and 2-D wavelet filter are used for feature extraction. This method is invariant to translation and rotation and is tolerant to illumination. The classification rate on using the Gabor is 98.3% and the accuracy with wavelet is 82.51% on the Institute of Automation of the Chinese Academy of Sciences (CASIA) database. In the approach proposed by [L. Ma,Y.Wang, and D. Zhang, 2004], multichannel and Gabor filters have been used to capture local texture information of the iris, which are used to construct a fixed-length feature vector. The results are FAR = 0.01% and FRR = 2.17% in CASIA database. Generally, unimodal biometric recognition systems present different drawbacks due its dependency on the unique biometric feature [Vincenzo Conti et al., 2010].

D. Limitations of Unimodal Biometric Systems

Most biometric systems deployed in real-world applications are unimodal, so they rely on the evidence of a single source of information for authentication. These systems have to contend with a variety of problems such as noise in sensed data, intra-class variations, inter-class similarities and spoof attacks [Salah M. Rahal et al., 2006].

Biometrics vs Passwords: First of all, the security of a password-based authentication tool such as ones in Unix or Windows systems are based on the local storage of only cryptographic hashes of passwords, no passwords themselves. This is possible because of the deterministic nature of password authentication: if the entered candidate password is the correct then its hash value equals the stored hash value and the authentication succeeds; if the entered candidate password is a wrong then its hash value differs and the authentication fails. Such an approach of security is impossible with biometric data.

Any new capture of a biometric candidate results in slightly different data which leads to the statistical nature of Biometrics based authentication (distance evaluation between two samples). The hash value of a reference biometric template will be totally different from the hash value of any matching candidate. This means that biometric references have to be stored in clear text.

A deep characteristics analysis of both passwords and biometrics shows a clear apposition:

- Secrecy: A password/PIN code is a secret, whereas biometric data is public. But have to make here a distinction between biometrics leaving traces (e.g. fingerprints) and others (e.g. hand geometry).
- Delegation: Depending on the application, the delegation ability is mandatory (banking, mobile communications) or must be impossible (civilian identification documents).
- Changeability: In case of compromise, a password is denied and another one is issued. It's not that easy with biometrics.
- Personalization: A PIN code is mailed (e.g. banking), whereas biometrics request user's Enrollment (i.e. the user has to go in a security area of the registration authority).
- Comparison process: The comparison between two PIN codes is a very simple task for a smart card, whereas comparing fingerprints needs far more computation resources.
- User convenience: A PIN code must be memorized and often manage several PIN codes, whereas biometrics need no effort.
- Vulnerability to eavesdropping: A discrete monitoring the actions could reveal the password, whereas biometric data cannot be copied.
- Vulnerability to brute force attack: Passwords are few characters long, whereas a biometric template is few hundreds of bytes.
- Countermeasures: Attacks against PIN code and passwords are experienced for many years and countermeasures are mature. Attacks against biometric systems is a novel area with no mature countermeasures for the time being.
- "Real" user authentication: User authentication with PIN code is only a legal trick: the law says "this PIN code is personal, do not share it". Biometrics is a stronger link with the user himself
- Capture: Entering a PIN code is simple (small keyboard), whereas capturing a biometric trait is an expensive task (cost and maintenance of a reader)

This opposition confirms the good complementarity of passwords and biometrics. The replacement of one with the other should be carefully studied depending on the targeted application. Despite the aforementioned vulnerabilities of biometrics, it should be counterbalanced with situations where biometrics is more secure than passwords: weak passwords, bad managed passwords, password-based authentication deactivated by the user.

Many information system administrators complain about users writing their password on a Post-It R note stuck under their keyboard or even on their computer's screen. Many mobile phone users leave the default PIN code (e.g. 0000, 1234) to unlock the phone or even deactivate this security feature considered as counter user convenient. Too many passwords, to be memorized, are short and explicit hence it could be easily guessed with simple dictionary attack or more sophisticated attacks. [Claude BARRAL 2010]. The various characteristics of biometric and password are listed in Table 2.

Table 2: Biometrics vs Passwords [Claude BARRAL 2010]

Characteristics	PIN code	Biometrics
Secrecy	Secret	Public
Delegation ability	Yes	No
Changeability	Yes	No
Personalization	Easy	Difficult
Comparison process	Simple	Not so trivial
User convenience	No	Yes
Vulnerability to Eavesdropping	Yes	No
Vulnerability to Brute Force attack	Yes	Not so trivial
Attacks countermeasures	Mature	Immature
"Real" user authentication	No	Yes
Capture	Easy	Expensive

III. RESULTS AND DISCUSSION

The biometric security system discusses the general classification of a biometric system and various mobile ad hoc network attacks. The three primary components of security such as authentication, authorization and accountability are used in the biometric security. The attacks can be classified into the five categories such as black hole, byzantine, wormhole, spoofing attack and Sybil attack. Cluster based intrusion detection and prevention technique, fingerprint and iris recognition are also discussed in biometric technology. The system also reviewed multimodal biometric schemes and four slap fingerprint scanner to simultaneously collect fingerprints of multiple fingers on a hand in one image.

REFERENCES

[1] Ashish Mishra., [2010], "*Multimodal Biometrics it is: Need for Future Systems*", International Journal of Computer Applications, Vol. 3, No.4, pp. 28 – 33.

[2] Aureli Soria-Frisch, Alejandro Riera and Stephen Dunne., [2010], "*Fusion Operators for Multi-modal BiometricAuthentication Based On Physiological Signals*", 978-1-4244-8126-2/10/$26.00 ©2010 IEEE.

[3] Bahgat S F, Ghoniemy S, and Alotabi M., [2013], "*Proposed Multimodal palm-veins- face Biometric Authentication", International journal of advanced computer science and applications*, Vol.4, No. 6.

[4] Besbes F, Trichili H and Solaiman B., [2008], "*Multimodal Biometric System Based on Fingerprint Identification and Iris Recognition*", in the Proceedings of 3rd Int. IEEE Conf. Inf. Commun. Technol.: From Theory to Applications (ICTTA 2008), DOI: 10.1109/ICTTA.2008.4530129, pp. 1 – 5.

[5] *Biometric Data Interchange Formats*—Part 6: Iris Image Data, ISO/IEC, 19794-6, Mar. 2004, draft Version, [Online].

[6] Ramalingam M and Thiagarasu V., [2014], "*Cluster Based Stretch and Shrink Method for Manet Using Load Balancing, Nearest Neighbor and Rule Mining*", International Journal of Engineering Sciences & Research Technology.

[7] Bo Yang, Ryo Yamamoto and Yoshiaki Tanaka., [2013], "*Dempster-Shafer Evidence Theory Based Trust Management Strategy against Cooperative Black Hole Attacks and Gray Hole Attacks in MANETs*", ICACT Transactions on Advanced Communications Technology(TACT), Vol. 2(3), pp. 223 – 232, May, 2013.

[8] Ramalingam M., Prabhusundhar P, Thiagarasu V, "*Biometric Based Intrusion Detection System using Dempster-Shafer Theory for Mobile Ad hoc Network Security*", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 5 Issue: 7, pp. 384 – 391, June-2017.

[9] Ramalingam M and Thiagarasu V., [2014], "*Cluster Based Stretch and Shrink Method for Manet Using Load Balancing, Nearest Neighbor and Rule Mining*", International Journal of Engineering Sciences & Research Technology, 3(10.): October, *2014*, ISSN: 2277-9655.

[10] Bolle. R., [1999], "*System and Methods for Determining the Quality of Fingerprint Images*", United States patent number US596356.

[11] Lim. E, Jiang. X and Yau. W., [2002], "*Fingerprint Quality and Validity Analysis*", in the proceedings of IEEE International Conference on Image Processing (ICIP '02), pp. 469 –472.

[12] M. Ramalingam, V Thiagarasu, "*Routing and Broadcasting in MANET: A comprehensive Analysis based on, Routing technique, Clustering and Architectural Model*", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, IJESRT 3 (11), November 2014.

[13] Lingxuan Hu D. E, [2005], "*Using Directional Antennas to Prevent Wormhole Attack*", 2005.

