Improving the Security of MANETs Oriented Military Intelligence using Biometrics Authentication Technologies

Julius N. Obidinnu [1] (obijulius@yahoo.com)
Ayei E. Ibor [2] (ayei.ibor@gmail.com)
S. O. O. Duke [3] (orokduke2003@yahoo.com)

[1, 2, 3]: Department of Computer Science,
Cross River University of Technology, Calabar, Nigeria

***Abstract*- In many parts of the world, the military has been very busy in recent times engaging in terror and other related wars. This requires that men and materials have to be located in different parts of their strategic geographic centres. And in order to ensure a fast communication with these bases, the military often deploys Mobile Ad-hoc Networks (MANETs). MANETs carry such intelligence information as: deployment information, readiness information, and order of battle plans to their various bases. The nature of these information is such that any compromise on them could be disastrous to the courses of action of the bases. This paper identifies user authentication as a key issue in strengthening security concerns in MANETs. The paper further adopts biometrics technologies as the trending options for the purpose of obtaining a truer reflection of the identities of the users of ad-hoc networks. This paper therefore, reviews various biometrics technology implementation strategies available, and recommends the adoption of one, or a combination of them by military bases. The benefits provided by this technology are also presented.**

***Index Terms*- Military Base, Biometrics Technology, Authentication, MANET, Information security**

I. INTRODUCTION

Most military bases require the use of Mobile Ad-hoc Networks (MANETs) to establish communications between the large numbers of mobile devices deployed in the battlefield [17]. It is therefore, instructive to state that the computer systems in military MANETs contain sensitive information, which often makes them attractive targets to unauthorised accesses. Tittel**,** Chapple and Stewart in [21] provide a list of some of the sensitive information, which also includes military descriptive intelligence such as: deployment information, readiness information, and order of battle plans. Illegal access to these classes of military intelligence could compromise investigations, disrupt military planning, and threaten national security. At all times therefore, it is crucial that the computer systems in military MANETs should be protected from intruders.

Consequently, this paper reviews one of the critical security protection steps that ensures that only authorised personnel gain access to the systems in the military MANETs. Consequently, we adopt the position of [15], who identifies user authentication as one of the key issues in managing security concerns in MANETs. And in the opinion of the referred author, access to ad-hoc networks is dynamic and context-sensitive, thereby making users' authentication to be on the fly with temporary access to resources. Accordingly, information leakage on military intelligence could occur in the process. These information leakages can be avoided. Therefore, [16] advocates that the exact identities of the users of the ad-hoc networks' should be accurately verifiable at any instance of its usage.

The advocacy in the preceding paragraph serves as the motivation for this paper, which reviews existing authentication processes, and identifies the biometrics technologies as the trending options for the purpose of obtaining a truer reflection of the identities of the users of ad-hoc networks. This paper therefore, reviews various biometrics technology implementation strategies available, and recommends the adoption of one or a combination of them by military bases.

II. IMPORTANCE OF AUTHENTICATION IN MILITARY MANETs

Wikipedia in [22] defines a mobile ad-hoc network (MANET) as a wireless, self-configuring, infrastructure-less network of mobile devices, deployed oftentimes for an interim purpose. And they are important to the military because they possess the features of quick setup, takedown, and mobility features. MANETs are therefore, especially useful to the military, since they serve as channels through which they communicate in order to strategize, command, control, and operate their forces in their respective environments, in land, sea, or air [20].

However, communications within MANET requires having legal access to the devices, as anything to the contrary will lead to information leakage on military intelligence to the opponents. And availability of military intelligence in the hands of an enemy is a bad omen for such a military base. Consequently, it becomes necessary to ensure that the identity of a person or device that attempts to gain access to the network should be authenticated. It is therefore, in line with this position that [20] identifies authentication as the first line of defence in securing MANET networks.

Authentication is any process by which a system verifies the identity of a user who wishes to access it [6]. Authentication is important in MANETs, as it ensures secure connections with a requesting entity into a network [2]. And authentication in

MANETs can be based on different mechanisms. We discuss these mechanisms in the next section.

III. AUTHENTICATION MECHANISMS

Allowing access to only authorised users and disallowing access to the unauthorised ones is a fundamental aspect of authentication. Authentication processes are based largely on three methods. These methods include:

- What we know – passwords, pin codes and other personal details can be used to identify users of a particular system
- What we have – tokens such as smartcards or key fob are also used for user authentication
- What we are – here, biometric features such as fingerprint scans, iris scans, palm biometrics are deployed for allowing access to controlled environments [23], [17], [16] and [12].

Authentication by 'what we know' and 'what we have' increases the likelihood of identity theft as the use of passwords or tokens is not necessarily tied to the identity of the real owner of the password or token [5]. In his study, [17] highlights that there are consequences attributed to setting up communication with a user that has an unknown identity. A knowledge factor such as a password is not entirely secure as it can be easily guessed, intercepted or transferred to another user [23]. In the event of User A divulging his authentication parameter such as a password to User B intentionally or accidentally, it will be difficult to capture the identity of the logged in user. More so, simple passwords can be easily guessed or cracked through brute force or dictionary attacks while complex ones can easily be forgotten. Though there are various mechanisms to protect passwords such as resetting them regularly or using passwords hints, authentication with the use of passwords is fast becoming problematic due to the sophisticated nature of technology and the pervasive Internet that allows access to all categories of information, some of which have far reaching impact on digital assets [3].

Nandini and RaviKumar in [14] describe 'what users have' as knowledge based authentication also called possession factors. Possession factors have found widespread usage in recent times, as they have added another level of security to authentication. Most of 'what users have' technologies are based on a two factor authentication mechanism, with PINs or passwords as secondary authentication features. Using a smart card or key fob, for instance, is a great way to enhance privacy. Most of the smart cards have the user's information engraved in them with peculiar attributes that maps the identity of the user to the card. Though this creates a sense of security for the numerous users across the globe, the use of tokens is subject to replay and active attacks [13], [25].

However, possession factors can be lost, stolen or damaged [12]. In such a situation, replacing them is necessary. But there is the possibility of using them to commit crime before they can be retrieved. This can create problems for the owner. Since a card owner may have his name engraved on a card, using it by a malicious user, if lost, will still record a transaction against the card owner. This is a serious security concern.

Let us assume that a smart card that grants access to a military database falls into the hands of an enemy soldier or group of soldiers. In the same vein, let us assume that this card belongs to a system administrator that has root or system privileges in a controlled system. The stated scenario can lead to severe consequences including divulgence of military intelligence, interception of military operations, distortion or deletion of sensitive classified data as well as loss of enormous digital assets such as files and even the complete database.

A more secured way of hardening the security of the system in this scenario is by deploying a mechanism that allows the use of the physiological features of the authorised user. Shan et al in [25] asserts that the use of biometrics is underpinned by measurable physiological traits and behavioural characteristics that serve as identity parameters for an individual. This assertion implies that the use of biometrics is not subject to authentication ills such as repudiation, impersonation and identity spoofing, since each individual's physiological traits are unique to the individual and are not transferable.

Chetty and Wagner in [3] agree that biometric authentication is becoming an inevitable aspect of information technology with the ubiquitous nature of computer systems and networks across the globe. As elaborated in [16], biometrics does not have to be remembered during the authentication process as they are inherent features of the individual that is being authenticated. This is in contrast to the use of passwords and tokens such as smart cards, which are subject to theft, sharing and loss ([12], [14].

Relatedly, Ichino and Yamazaki in [8] discuss the efficacy of biometric authentication specifically underpinned by soft biometrics. In the study, they classified soft biometrics on the basis of facial, body and accessory traits. Furthermore, they assert that, though soft biometrics may not be distinctive enough to identify individuals uniquely, it can be valuable for enhancing biometric authentication through the categorisation of the collected traits, such as eye colour and height ranges.

In the same way, [18] investigates the robustness of biometrics for identity verification and access control. Since biometric features are intrinsic to the individual they identity, they posit that forgetting or forging them like passwords or documents is unlikely. Their analysis of secure biometrics was leveraged by the design of an appropriate training procedure for matching a stored biometric signal with a probe for onward decision making during authentication.

Similarly, [1] proposed an encrypted iris authentication system for identifying and authenticating users of a wireless sensor networks. Most military operations are dependent on the deployment of wireless sensor networks (WSNs) for command and control. Since WSNs are simple to implement and manage, using biometrics for identification and authentication processes will enforce a highly secure access control system on the fly. Authentication through physiological traits such as finger touches, face movement or palm print was discussed for payment systems in [10]. This method of making payments can be enhanced to allow for secure authentication processes in military sites. Multimodal

biometric authentication is also important for enhancing operational security.

As discussed in [5], multimodal biometrics is suitable for mobile devices including Personal Digital Assistants (PDAs), smart phones and mobiles phones. Since these devices are portable, they are subject to loss and theft. Protecting them, therefore, requires the use of an enhanced security mechanism such as biometric authentication. They proposed the use of teeth image and voice for authentication. It is a known fact that the military deploys the largest use of mobile devices, most of which are embedded systems with tactics and military intelligence. If authentication to such devices is leveraged by teeth image and voice, it will become computationally difficult to circumvent the security of such a device in the event of its loss, theft or misplacement.

Biometric authentication, therefore, is more secure in access control management as well as identity verification especially for controlled domains where the exact identity of the user being authenticated and allowed access to digital resources cannot be compromised.

IV. APPLICABLE BIOMETRIC TECHNOLOGY

The biometric technology is leveraged by a number of methodologies that can be deployed in the realisation of biometric authentication. Some of these, as discussed in [7] and [17] include the following:

a. Palm biometrics
b. Fingerprint authentication
c. Voice recognition
d. Signature verification
e. Iris scan and
f. Facial recognition

All of these are necessary. However, this paper focuses on the first three above: palm biometrics, fingerprint authentication and voice recognition.

A. Palm Biometrics

Palm biometrics is based on the use of biometric traits extracted from the palm (curvature of the palm, width of the palm, length of fingers, thickness of the palm, principal lines, wrinkles, delta points etc [7]) to verify the identity of a person in a controlled environment. The use of palm biometrics, on itself, cannot guarantee an efficient user identification system without being augmented by other identification methods such as the use of personal identification numbers (PIN) as the human hand is not unique. The reliability provided by palm biometrics in the context of verification and authentication is considerably high. Non repudiation is enhanced as a user cannot deny that a physiological trait such as a palm print image does not belong to him/her once logged in. Tracking users' access and the use of resources can be controlled. Also, there is more convenience for users and system administrators as incidences of password or identification card theft or loss may not be obtainable thereby enhancing efficiency.

Some of the key weakness of palm biometrics is that the sensor data, if used independently of other biometric sources, can be noisy. Also, the human hand is not completely unique and as such may lack individuality and universality in representing the identity of a particular individual. Injuries on the palm as well as gummy palms may lead to poor template quality culminating in poor performance by the biometric system. Palm biometrics should therefore be used in combination with other biometric sources such as fingerprints, iris scans and voice recognition to provide an efficient multimodal authentication system. Though palm biometrics demonstrates some weaknesses in its implementation, it has a good number of strengths as follows:

i. It can be suitable for outdoor environments such as military sites and can be used to manage a high throughput of people.
ii. It provides a friendly user interface that is robust and integrates easily with the existing as well as third party systems.
iii. Gives room for easy maintenance and storage as it has a small template size that can be integrated in a large database.
iv. It is inexpensive to implement and offers excellent return on investment as well as widespread acceptance.
v. Highly reliable and accurate.
vi. It provides effective security, which is more robust when compared to traditional methods such as the use of passwords and identification cards.
vii. Since the biometric features extracted during enrolment are inherent to a particular individual, fraud and repudiation can be eliminated during authentication. This may not be unconnected with the fact that once stored, palm biometric traits are not transferable; that is, they cannot be shared, stolen, lost or forgotten.

B. Fingerprint Authentication

There is a proliferation in the use of fingerprint authentication in recent times [11], [4]. This can be seen in most mobile phone service providers. The use of fingerprints for identification and verification is borne out of the fact that the patterns of ridges and furrows that characterise an individual's finger (most especially the surface of the fingertip) are unique to each individual [23], [9]. Fingerprint devices allow a user to access a controlled environment through fingerprint scans. Podio in [16] maintains that the user merely places his finger tip on the appropriate device to be identified and authenticated. This paves way for secure access control and network authentication mechanism. However, fingerprint biometrics can be given to the weaknesses of palm biometrics especially when there is an accumulation of skin oils or dirt on the surfaces of sensor plates. The resultant effect may be false rejection in which case a valid user fingerprint scan is rejected as illegitimate. False acceptance can also be obtainable here where an invalid fingerprint scan is accepted as valid for a given user transaction [7].

C. Voice Recognition

Voice recognition is based on the distinct rate and pitch of sounds produced by the human voice [19], as well as other

acoustic features of speech including the shape of the throat, speaking style and size of the mouth [16]. Kounoudes et al in [12] mention that voice authentication is preceded by the extraction of voiceprints, which are stored during the enrolment phase and matched with raw speech data captured by voice recognition devices such as a voice speaker or microphone.

Xiao in [17] identifies two types of technologies for voice biometrics namely voice scans and speech recognition. The main distinction between the two technologies is that while voice scans use a pre-stored voice sample of the user to authenticate and verify the identity of the user, speech recognition depends on words and sentences from an audio signal, which form the input to a voice recognition device.

Zhang and Abdulla in [24] proposed a voice biometrics technique based on human auditory models and independent component analysis. The auditory models were found to achieve better identification rates with high robustness to noise. Furthermore, Rashid et al in [19] implemented a security system that allows for voice patterns as the access control key thereby enhancing the accuracy of the authentication process since voice patterns as seen to be distinct per individual. The design of the proposed auditory models, access control mechanism, and voice recognition system is suitable for deployment in military controlled environments.

One major advantage of voice biometrics is that it does not require physical contact with the authenticating device though it can be subject to background noise, which may lead to a high rate of false rejection [12]. However, voice templates, as highlighted in [16] are small in size basically less than 16 kilobytes and can be represented using neural networks, decision trees, pattern matching algorithms and hidden Markov models.

V. BIOMETRIC AUTHENTICATION PROCESS

Biometric authentication is preceded by an enrolment procedure. The enrolment process requires the initial capture of the biometric traits. As stated in [11] and [23], the captured traits are pre-processed for feature extraction and stored as templates in the authenticating device or database. The performance of the biometric sample during authentication is dependent on the quality of the captured template. Figure 1 is a representation of a Biometric Authentication Process.

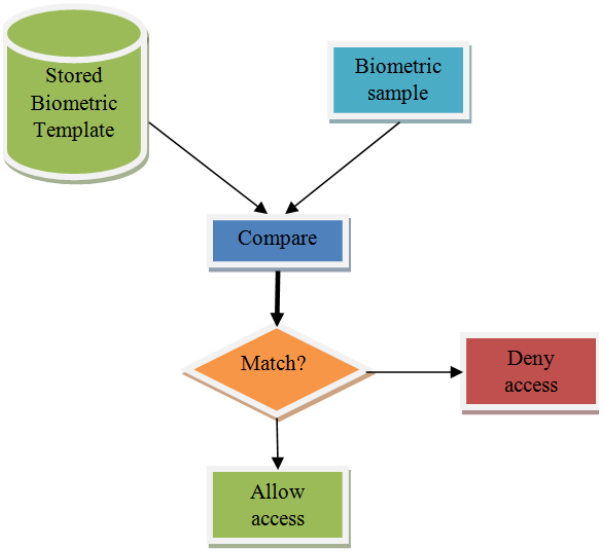

Fig. 1: Representation of a Biometric Authentication process

Verification is an indispensable aspect of biometric authentication [16]. A user whose biometric sample has been enrolled can only be allowed access to a system such as during a login session by verification. During verification, the stored biometric template is compared with the sample presented by the user at the point of authentication. Access is allowed when a match is found and in the event of a mismatch, access is denied. Verification leads to identification and usually involves a one-to-many or one-to-one matching of the stored template in the database with the captured sample [25].

VI. CONCLUSION

One of the key issues in managing a user's access to critical resources is the ability to allow only the authorised users of a system to such resources. Over the years, identity spoofing, man in the middle, replay and active attacks have left most military bases prone to the leakage of classified information and intelligence as well as the circumvention of established security procedures. The consequences of security breaches are grave and can lead to loss of lives, property and revenue. As seen in most third world counties, where terrorism is on the increase, leakage of sensitive information can cripple the bedrock of an economy. To this end, providing adequate and enhanced authentication mechanisms to controlled environments cannot be overemphasised.

One can vividly assess that authentication through a user's physiological features can create a sense of security. This is because the physical presence of the user including an aspect of his traits will be involved in identifying him. Biometric traits are invariant in representation and as such claim a certain degree of uniqueness and universality. The fingerprint image of one user cannot be used in the place of another user. This is a universal truth. Consequently, it is highly efficient to deploy biometric authentication if the system administrator is interested in mapping the users of a system to their real identities.

Password and token authentication cannot guarantee non-repudiation. We cannot claim that a user who logs into a

system is the owner of the password or token such as smart card used to gain access to the system. Passwords and tokens can be lost, stolen, and are also transferable. With biometric authentication, such weaknesses can be controlled since the users' physiological and behavioural traits are unique, which requires the physical presence of the user at the point of authentication leveraged by the use of live biometric samples for identification and verification.

This paper has been able to highlight the efficacy of biometric authentication in critical environments such as the military. The focus on future work should be on biometric template security. This is borne out of the fact that a compromised biometric template, which is intrinsically invariant, can lead to the construction of artificial biometric templates through reverse engineering if such a template falls into the hands of a malicious user.

REFERENCES

[1] Althobaiti, O.; Al-Rodhaan, M.; Al-Dhelaan, A., (2012) "Biometric access control for wireless nodes," Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on , vol., no., pp.167,174, 21-23

[2] Balfanz, D., Smetters, D. K., Stewart, P., and Chi Wong, H. (2002). Talking To Strangers: Authentication in Ad-Hoc Wireless Network, Proceedings of Network and Distributed System Security Symposium 2002 (NDSS'02), San Diego, CA, February, 2002.

[3] Chetty, G.; Wagner, M., (2006) "Multi-Level Liveness Verification for Face-Voice Biometric Authentication," Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session, vol., no., pp.1,6

[4] Darwish, A.A.; Zaki, W.M.; Saad, O.M.; Nassar, N.M.; Schaefer, G., (2010) "Human Authentication Using Face and Fingerprint Biometrics," Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference on , vol., no., pp.274,278

[5] Dong-Ju Kim; Kwang-Seok Hong, (2008) "Multimodal biometric authentication using teeth image and voice in mobile environment," Consumer Electronics, IEEE Transactions on , vol.54, no.4, pp.1790,1797

[6] Hitachi ID Systems Inc. (2014). Definition of Authentication. Available at: http://hitachi-id.com/concepts/authentication.html (Accessed: 12 January 2014)

[7] Yan, H. & Long, D. (2008) "A Novel Bimodal Identification Approach Based on Hand-Print," Image and Signal Processing, 2008. CISP '08. Congress on , vol.4, no., pp.506,510

[8] Ichino, M.; Yamazaki, Y., (2013) "Soft Biometrics and Its Application to Security and Business," Biometrics and Kansei Engineering (ICBAKE), 2013 International Conference on , vol., no., pp.314,319

[9] Isa, M.R.M.; Yahaya, Y.H.; Halip, M.H.M.; Khairuddin, M.A.; Maskat, K., (2010) "The design of fingerprint biometric authentication on smart card for PULAPOT main entrance system," Information Technology (ITSim), 2010 International Symposium in , vol.3, no., pp.1,4

[10] Yang, J. (2010) "Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System," Management of e-Commerce and e-Government (ICMeCG), 2010 Fourth International Conference on , vol., no., pp.405,410

[11] Kannavara, R.; Bourbakis, N.G., (2009) "Fingerprint biometric authentication based on local global graphs," Aerospace & Electronics Conference (NAECON), Proceedings of the IEEE 2009 National , vol., no., pp.200,204

[12] Kounoudes, Anastasis; Kekatos, V.; Mavromoustakos, S., (2006) "Voice Biometric Authentication for Enhancing Internet Service Security," Information and Communication Technologies, 2006. ICTTA '06. 2nd , vol.1, no., pp.1020,1025

[13] Dang, L., Kou, W., Xiao, Y. (2005) "An improved scheme for unilateral asymmetric smart card authentication," Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on , vol.2, no., pp.265,268 vol.2

[14] Nandini, C.; RaviKumar, C. N., (2007) "Multi - Biometrics Approach for Facial Recognition," Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on , vol.2, no., pp.417,422

[15] Ngai, E.C.-H.; Lyu, M.R.; Chin, R.T., (2004) "An authentication service against dishonest users in mobile ad hoc networks," Aerospace Conference, 2004. Proceedings. 2004 IEEE , vol.2, no., pp.1275,1285 Vol.2

[16] Podio, F.L., (2002) "Personal authentication through biometric technologies," Networked Appliances, 2002. Gaithersburg. Proceedings. 2002 IEEE 4th International Workshop on , vol., no., pp.57,66

[17] Xiao, Q. (2004) "A biometric authentication approach for high security ad-hoc networks," Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC , vol., no., pp.250,256

[18] Rane, S.; Ye Wang; Draper, S.C.; Ishwar, P., (2013) "Secure Biometrics: Concepts, Authentication Architectures, and Challenges," Signal Processing Magazine, IEEE , vol.30, no.5, pp.51,64

[19] Rashid, R.A.; Mahalin, N.H.; Sarijari, M.A.; Abdul Aziz, A.A., (2008) "Security system using biometric technology: Design and implementation of Voice Recognition System (VRS)," Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on , vol., no., pp.898,902

[20] Tang, H., Salmanian, M. & Chang, C. (2007). Strong Authentication for Tactical Mobile Ad Hoc Networks. Defence Research and Development Canada Ottawa TM 2007-146

[21] Tittel, E., Chapple, M. & Stewart, J. M. (2003). Certified Information Systems Security Professional. CA: SYBEX Inc.

[22] Wikipedia (2014). Mobile ad hoc network. Available at: http://en.wikipedia.org/wiki/Mobile_ad_hoc_networks (Accessed: 11 January 2014).

[23] Yahaya, Y.H.; Isa, M.; Aziz, M.I., (2009) "Fingerprint Biometrics Authentication on Smart Card," Computer and Electrical Engineering, 2009. ICCEE '09. Second International Conference on , vol.2, no., pp.671,673

[24] Zhang, Y. & Abdulla, W.H., (2008) "Voice as a Robust Biometrics," Future Generation Communication and Networking, 2008. FGCN '08. Second International Conference on , vol.3, no., pp.41,46

[25] Shan Ao; Weiyin Ren; Shoulian Tang, (2008) "Analysis and Reflection on the Security of Biometrics System," Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference, vol., no., pp.1,5