International Journal of Engineering &Technology, 7 (4) (2018) 6731-6734

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.19020
Research paper

Securing WSN and MANET communication for military operation based on ECC algorithm

Mohd Rizal Mohd Isa [1] *, Muhammad Naim Abdullah [1], Omar Zakaria [1], Mohd Nazri Ismail [1], Mohammad Adib Khairuddin [1], Kamaruzaman Maskat [1], Mohd Afizi Mohd Shukran [1], Mohd Fahmi Mohamad Amran[1]

[1] Faculty of Science & Defence Technology, Universiti Pertahanan Nasional Malaysia, MALAYSIA
**Corresponding author E-mail: rizal@upnm.edu.my*

Abstract

The key aspect in military operations is keeping the communication stable and secure as possible. Connection downtime should be avoidance as it creates miscommunication between Military officers hence would impact on the targeted mission. The complexity of the terrains such as in the jungle area, contribute to a great challenge in maintaining the communication amongst military officer. Wireless Sensor Network (WSN) and Mobile Ad-Hoc Network (MANET) have been chosen to support on the communication platform between military officers for its capability in maintaining the stability of the connection lines. The confidential of the shared data amongst the military officers are also crucial which could be stolen and tampered by outsiders. The Elliptic Curve Cryptography (ECC) algorithm is selected for its ability to provide high security with small key size. This paper proposed a new framework in securing the WSN and MANET communication based on ECC algorithm for Military operations. The contribution of this research will not only towards military operations but not limited to Search and Rescue (SAR) operations as well.

Keywords: *Wireless Sensor Network; Mobile Ad-Hoc Network; Elliptic Curve Cryptography; Military; Search and Rescue.*

1. Introduction

In the near future, soldiers would be equipped with advanced integrated sensors including integrated day/night thermal, temperature and humidity sensor for health monitoring and living status, advanced training and simulation (extracted from tacit knowledge of military operations) (P.N.E Nohuddin, M.R.M. Isa & M.A.M. Shukran. (2012)) and GPS sensor for soldiers or SAR real time position tracking status from base camp. In addition, he will be protected with integrated secure communication gear, lightweight body armour that defends against chemical and biological weapons. All of this equipment is powered from long life time batteries or capacitor which could be draw power from its environments and attached to his backpack (see Figure 1).



Fig. 1: The Future Soldier's Gears.

The issue of getting the message across military officers securely in the complex environment is a challenge. As the data travel wirelessly, it gave freedom for outsiders to capture the transmission of data. An enemy or outsider could be in a hidden areas running eavesdropping or packet sniffing activity. In military operation, military officer shares sensitive data amongst each other such as on their next actions or strategies. Figure 2 illustrates the proposed framework of wireless sensor network /mobile ad-hoc network for military and SAR operations (A.K.A. Ghani, M.N. Ismail, Z. Omar, & P.N.E. Nohuddin. (2016); N.J. Wesenten, G. Belenky, & T.J. Balkin. (2005)). As the data travels in Cleartext form (as shown in Figure 2 below), there is necessities in protecting the data with encryption technique. Thus, the objectives of this research is to proposed a framework to protect the communications for military and SAR operations.

The rest of the paper is organized as follows. In section 2, we reviewed the related works on WSN/MANET application. Section 3, is the methodology where we discussed ECC as the adapted public key cryptography for the proposed framework. Section 4 is the layout of the proposed framework in securing the WSN/MANET for military and SAR operations. Lastly, in section 5 is the conclusion where we summarized the importance of the research.

2. WSN in military applications

WSN are widely used because of their tiny and compact size and ease of installation. Hence, it is not surprise that it is being used in many areas such as below:

Copyright ©2018 Mohd Rizal Mohd Isa et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Public safety: WSN help in determining presence of weapons, explosive materials, gas leakage at public places such as airports, sport stadium, concerts arena and theme parks.
Automation industry: The main concerns with heavy and large machines is to maintain its part from sudden broke out. Therefore, these machines are embedded with sensors to run diagnosis and alert the management whenever the maintenance is required.
Personal belongings: WSN is use in tracking the current location of personal possessions such as vehicles and devices.
Medical applications: Home and elderly care centre monitoring for chronic and elderly patients. WSN enable for remote monitoring of patients and their vital parameters.
There are various studies of WSN implementation in military environment including discovery of explosive mines, enemy monitoring and target classification, battlefield surveillance, battlefield damage assessment, detection of Nuclear Biological Chemical (NBC) attacks (F. Khan & K. Nakagawa. (2012)) and Knowledge Management (KM) amongst military officers or SAR personal on a mission (P.N.E Nohuddin, M.R.M. Isa & M.A.M. Shukran. (2012); A.K.A. Ghani, M.N. Ismail, Z. Omar, & P.N.E. Nohuddin. (2016)).
Some authors have proposed mine detection systems to determine the area which contains explosive mines (D. Puthal, S. Nepal, R. Ranjan, & J. Chen. (2015); D. Puthal, S. Nepal, R. Ranjan, & J. Chen. (2016); D. Puthal & B. Sahoo. (2012); D. Puthal & B. Sahoo. (2012); M. A. Jan, P. Nanda, M. Usman & X. He. (2016)). WSN helps in the discovery of mines in the affected area by deploying a number of smart sensing devices in a heterogeneous environment and alert the forces. These sensing devices capture a variety of data and send them to the server for analysis as data streams. There are also WSN application in battlefield surveillance (F. Khan, S.A. Kamal & F. Arif. (2013); M. A. Jan, P. Nanda, X. He and R. P. Liu (2013); Q. Jabeen, F. Khan, S. Khan & M.A. Jan. (2016); F. Khan, & K. Nakagawa (2013)) mainly in closely monitored restricted areas and borders F. Khan, & K. Nakagawa (2012). The embedded sensors obtain any information on enemy activities and provides time for faster response and decision making (M. Usman, M. A. Jan & X. He. (2016). WSN also useful for enemy monitoring such as spotted sniper hidden position (M. A. Jan, P. Nanda, X. He, Z. Tan & R. P. Liu. (2104)) and tracking military vehicles (M. A. Jan, P. Nanda & X. He (2013); Ananyachatterjee, ManjushaPandey. (2014)); G. Simon, M. Maróti, Á. Lédeczi, G. Balogh, B. Kusy A. Nádas, G. Pap, J. Sallai & K. Frampton. (2004); Ms. Sunita, J. Malik, SumanMor. (2012); K. Romer & F. Mattern. (2004). In addition, WSN can be used to locate enemy presence and inform the enforcement to send help to that particular area especially in urban areas to preserve its peaceful environment.

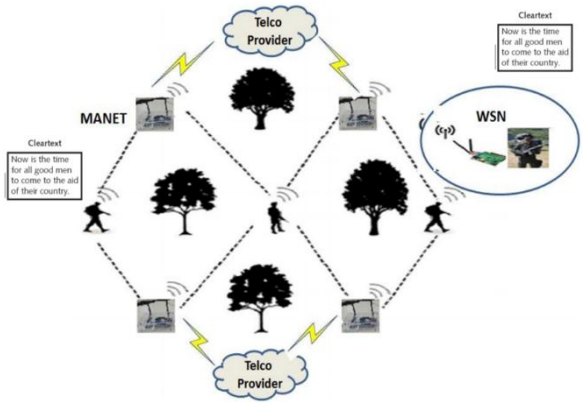


Fig. 2: The Framework of WSN/MANET Communication in Military and SAR Operation.

3. Method the proposed framework

Elliptic Curve Cryptography (ECC) is a public key (asymmetric) cryptography technique. Public key cryptography involves with two different keys, one for encryption and the other for decryption. Therefore, it is much secure that private key (symmetric) cryptography where only a single key is use for encryption and decryption process. ECC is considered as amongst the most popular public key cryptography algorithm alongside Rivest-Shamir-Adleman (RSA) algorithm (P. G. Shah, X. Huang & D. Sharma. (2010).
ECC is based on mathematical calculation of elliptic curves over finite fields (I.F. Akyildiz, W. Su, Y. Sankarasubramaniam & E.Cayirci (2002)) and it was proposed in 1985 by Neal Koblitz and Victor Miller. The main advantages of ECC compared with others algorithm is the key size. ECC is able to provide similar cryptographic strength as RSA with much smaller key size (Computer Security Division Information Technology Laboratory Transitions (2011)). As shown in the table below, ECC offers the same level of security with only 256 bits' key sizes whereas RSA demands a key length of 3072 bits for medium period security.

Table 1: Comparison between ECC and RSA on Key Size

ECC key sizes (Bits)	RSA key sizes (Bits)	Keysize Ratio (Bits)	Security Length
160	1024	1:6	Short period
256	3072	1:12	Medium period
384	7680	1:20	Long term period

The strength of all cryptography algorithm depends on a mathematical operation that is hard to crack its pattern. The equation of ECC is defined as below:

$$y^2 = x^3 + ax + b \tag{1}$$

where a and b are integers which gives a different elliptic curve to satisfy $4a^3 + 27b^2 \neq 0$ The first step, an elliptic curve and a base point p which lies on the curve must be known for every nodes in the network. Assume that to generate a shared key between two nodes, A and B, A select a random prime integer k_A and B pick a random prime integer k_B. k_A and k_B are the private keys of A and B, respectively. The public keys $\overline{k_A}$ and $\overline{k_B}$ of each node A and B is generated using the following equations:

$$\overline{k_A} = k_A \times p \tag{2}$$

$$\overline{k_B} = k_B \times p \tag{3}$$

Both A and B are the public keys of curve points. The private keys k_A and k_B specify the times of multiplying the base point p by itself to generate the public keys. A shared secret key R is generated by multiplying public keys with their private keys as in equation (4).

$$R = k_A \times \overline{k_B} = K_B \times \overline{k_A} \tag{4}$$

With only the values of $\overline{k_B}$, $\overline{k_A}$, and p, it is difficult for an eavesdropper to compute k_A and k_B which are the private keys of A and B. Hence, attackers cannot figure out the shared secret key R.
With ECC offered smaller key sizes, but with greater security therefore it is much applicable for WSN and MANET. As WSN and MANET devices only equipped with limited storage or processing power make ECC more appropriate to be adopted particularly in The Internet of Things (IoT) platforms. Figure 3 shows the proposed framework of securing the WSN and MANET in military and SAR operations using ECC algorithm.
A thorough research on the implementation of ECC for securing WSN/MANET is carried out and we have found only few research have proposed ECC as a solution to protect the WSN/MANET communication and until now, none of the researchers proposed a framework in protecting the WSN/MANET using ECC particularly for military application. Hence, the contribution of this pro-

posed framework are significant and beneficial not only limited to military and SAR operations but also could be enhance for other applications.

4. Conclusions

In this paper, a framework of securing the WSN and MANET communication for military and SAR operations is presented. As IoT falls under one of the focussed area in Fourth Industrial Revolution (4IR), it is relevant to implement WSN and MANET to military sector today. In WSN/MANET infrastructure, the issue of protecting the data transfer between nodes are crucial especially in military operations as the data involved are confidentiality and integrity. ECC is the perfect choice to secure WSN/MANET for several advantages such as its highest strength but lesser bit in

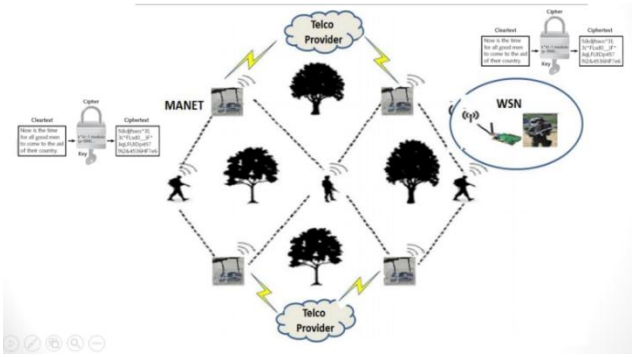


Fig. 3: The Proposed Framework on Securing WSN and MANET for Military and SAR Operations.

Current public key cryptosystems, its fast encryption and signature speed and its small signatures & certificates. Therefore, with the advantages mentioned above, the shorter keys management means lower storage space and faster arithmetic operations (less processing power) which made ECC as excellent choice for WSN/MANET.

Acknowledgements

This research work is supported by Ministry of Education, Malaysia under Niche Research Grant Scheme (NRGS) Project 3 – UPNM/2016/GPJP/4/ICT/3.

References

[1] P.N.E Nohuddin, M.R.M. Isa & M.A.M. Shukran. (2012). 'Information Technology Knowledge Management in Malaysian Armed Forces'. Journal of Convergence Information Technology 7 vol. (6). https://doi.org/10.4156/jcit.vol7.issue6.22.

[2] A.K.A. Ghani, M.N. Ismail, Z. Omar, & P.N.E. Nohuddin. (2016). 'Establishing mesh network amongst infantry personnel during military operations: A preliminary study'. 2016 International Conference on Information and Communication Technology (ICICTM), IEEE 16th - 17th May 2016, Kuala Lumpur, Malaysia. https://doi.org/10.1109/ICICTM.2016.7890804.

[3] N.J. Wesenten, G. Belenky, & T.J. Balkin. (2005). '*Cognitive Readiness in Network-Centric Operations*', Parameters, spring 2005, PP, 94-105.

[4] F. Khan & K. Nakagawa. (2012). Performance Improvement in Cognitive Radio Sensor Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE), 8.

[5] D. Puthal, S. Nepal, R. Ranjan, & J. Chen. (2015). A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream. In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing. https://doi.org/10.1007/978-3-319-26187-4_7.

[6] D. Puthal, S. Nepal, R. Ranjan, & J. Chen. (2016). A dynamic prime number based efficient security mechanism for big sensing data streams. Journal of Computer and System Sciences. https://doi.org/10.1201/9781315154008-13.

[7] D. Puthal & B. Sahoo. (2012). Secure Data Collection & Critical Data Transmission in Mobile Sink WSN: Secure and Energy efficient data collection technique.

[8] D. Puthal & B. Sahoo. (2012). Effective Machine to Machine Communications in Smart Grid Networks. ARPN J. Syst. Softw. © 2009-2011 AJSS Journal, 2(1), 18-22.

[9] M. A. Jan, P. Nanda, M. Usman & X. He. (2016). "PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks," "accepted", 2016. https://doi.org/10.1002/cpe.3986.

[10] F. Khan, S.A. Kamal & F. Arif. (2013). Fairness Improvement in long-chain Multi-hop Wireless Adhoc Networks. International Conference on Connected Vehicles & Expo (pp. 1-8). Las Vegas: IEEE Las Vegas, USA. https://doi.org/10.1109/ICCVE.2013.6799854.

[11] M. A. Jan, P. Nanda, X. He & R. P. Liu (2013). "Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013. https://doi.org/10.1109/HPCC.and.EUC.2013.198.

[12] Q. Jabeen, F. Khan, S. Khan & M.A. Jan. (2016). Performance Improvement in Multihop Wireless Mobile Adhoc Networks. in the Journal Applied, Environmental, and Biological Sciences (JAEBS), vol. 6(4S), pp. 82-92. Print ISSN: 2090-4274 Online ISSN: 2090-4215, TextRoad.

[13] F. Khan, & K. Nakagawa (2013). Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks. in IEEE World Congress on Communication and Information Technologies (p. 8). Tunisia: IEEE Tunisia. https://doi.org/10.1109/WCCIT.2013.6618728.

[14] F. Khan, & K. Nakagawa (2012). Performance Improvement in Cognitive Radio Sensor Networks. in the Institute of Electronics, Information and Communication Engineers (IEICE), 8.

[15] M. Usman, M. A. Jan & X. He. (2016). "Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds," Elsevier Information sciences, "accepted", 2016. https://doi.org/10.1016/j.ins.2016.08.059.

[16] M. A. Jan, P. Nanda, X. He, Z. Tan & R. P. Liu. (2104). "A robust authentication scheme for observing resources in the internet of things environment" in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE. https://doi.org/10.1109/TrustCom.2014.31.

[17] M. A. Jan, P. Nanda & X. He (2013). "Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN," in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013. https://doi.org/10.1007/978-3-642-38401-1_12.

[18] Ananyachatterjee & ManjushaPandey. (2014). "Practical Applications of Wireless Sensor Network Based on Military, Environmental, Health and Home Applications: A Survey"; International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January2014, ISSN 2229-5518.

[19] G. Simon, M. Maróti, Á. Lédeczi, G. Balogh, B. Kusy A. Nádas, G. Pap, J. Sallai & K. Frampton. (2004). "Sensor Network-Based Counters niper System"; SenSys'04 Proceedings of the 2nd international conference on Embedded networked sensor systems, Baltimore, USA, November 2004ISBN: 1- 58113-879-2 https://doi.org/10.1145/1031495.1031497.

[20] Ms. Sunita, J. Malik & SumanMor. (2012)." Comprehensive Study of Applications of Wireless Sensor Network"; International Journal of Advanced Research in Computer Science and Software Engineering;Volume 2, Issue 11, November 2012; ISSN: 2277 128X.

[21] K. Romer & F. Mattern. (2004). "The Design Space of Wireless Sensor Networks"; IEEE Wireless Communications, Volume: 11, Issue: 6, pp. 54-61, December 2004, ISSN: 1536-1284. https://doi.org/10.1109/MWC.2004.1368897.

[22] M. Kassim, C.K.H.C.K. Yahaya & M.N. Ismail. (2010). 'A prototype of web based temperature monitoring system'. Proceedings of the IEEE, International Conference on Information and Network Technology, June 22-24, 2010, Shanghai, China, pp: 266-270. https://doi.org/10.1109/ICETC.2010.5530066.

[23] M. Kassim, C.K.H.C.K. Yahaya & M.N. Ismail. (2010). 'A study on automated, speech and remote temperature monitoring for modeling web based temperature monitoring system'. Proceedings of the IEEE, International Conference on Information and Network Technology, June 22-24, 2010, Shanghai, China, pp: 229-233.

[24] M. T. Ismail, M.N. Ismail, S. S. Sameon, Z. M. Zin & N. Mohd. (2016). 'Wireless Sensor Network: Smart greenhouse prototype with smart design', 2016 2nd International Symposium on Agent,

Multi-Agent Systems and Robotics (ISAMSR), 2016, pp. 57-62. https://doi.org/10.1109/ISAMSR.2016.7810003.

[25] M.N. Ismail. (2012). 'Early fire detection: development of temperature sensor device in smart home monitoring system using mobile phone'. International Journal of Academic Research (IJAR), Part A; 4(5), 41 -49, 2012. https://doi.org/10.7813/2075-4124.2012/4-5/A.4.

[26] P. G. Shah, X. Huang & D. Sharma. (2010). "Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor networks", 2010 IEEE 24th International Coiference on Advanced Iiformation Networking and Applications Workshops. https://doi.org/10.1109/WAINA.2010.47.

[27] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam & E.Cayirci (2002). "Wireless sensor networks: a survey" Published by Elsevier Science B.V., 2002. https://doi.org/10.1016/S1389-1286(01)00302-4.

[28] Computer Security Division Information Technology Laboratory Transitions (2011). "Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" Computer Security Division Information Technology Laboratory: U.S. Department of Commerce, 2011.