ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 10, March 2017

A ANONYMOUS AUTHENTICATION PROTOCOL FOR SECURE DATA ACCESS FOR WIRELESS SENSOR NETWORKS

[1]Suzanna Charly, [2]Dr.Y. Harold Robinson
[1] PG Student, [2]Associate Professor, SCAD College of Engineering & Technology.

Abstract:

This project concentrates on WSN's critical security issue due to their unattended and hostile deployment in the field. Sensors are usually deployed for sensing task and to sink in the single hop topology. The sensed data is transmitted in multi hop or direct relaying manner. In model of energy consumption it cost less energy in shorter range than longer one. However, due to the nature of the sound wave, the concurrent transmission is the major issues in medium access control (MAC). This MAC also has a issue in data collisions sensor networks which is to be avoided. Authenticating remote users in such resource-constrained environment is a paramount security concern. At this time interval the slot owner hold isolated access rights. This gives a collision free communication and they do not have energy wasting contention period. User authentication in wireless sensor networks

Keywords- User Authentication, Wireless Sensor Networks, Security, RSA Algorithm.

I.INTRODUCTION

The rapid development of the micro electromechanical equipment system and wireless network technologies, wireless sensor networks (WSNs) are becoming more and more popular in day today life as they offer economically viable, real-time monitoring solutions. In hostile environment the wireless sensor can be done easily. They are used in hostile environment mostly. They are used is various fields like traffic monitoring, wildlife monitoring, health care monitoring, military surveillance, environment control, habitat monitoring and vehicle tracking,. This WSN plays a vital role in our daily life part. The external users on critical applications they commonly uses real time applications.

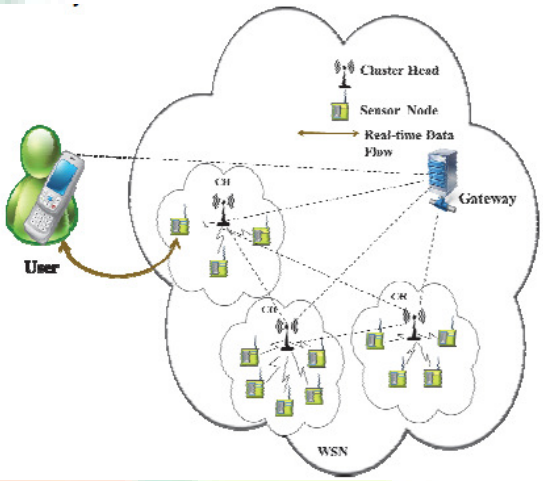
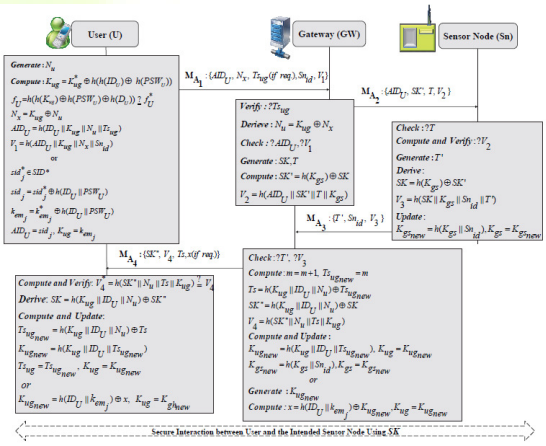


Fig. 1. Data Access in WSN's

The long delays of response the authentication introduce another kind of problem.

As shown in Fig. 2, at the beginning, all nodes are listening to the control channel. Node a starts its handshaking process with node b on the control channel and then selects channel 1 for communication. Later, nodes c and d also negotiate on the control channel for their data transmission. The CTS message is return to c node when the node b gives CTS message to node d and selects its own data channel .In this case, node d does not know that the channel has already been used by node b. Here is makes collision by communicating with c node with one channel. This is called as "long delay problem".



ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 10, March 2017

Fig. 2. Authentication and Key Exchange Protocol

User anonymity is among the imperative properties of two factor authentication schemes for WSNs. A more satisfactory property of user anonymity is user un-traceability. That is, a scheme accomplishing this advance property can resist the adversary from linking multiple instances of communication generated by the same user and also from tracing a current location, moving history, etc. As a consequence, most schemes that attempts to preserve user privacy aim at fulfilling this stronger notation of user anonymity.

II. SYSTEM MODEL

In this paper, we use the following multichannel WS network model: There are many channels in the network, where each has equal bandwidth. The control message exchange is dedicated by one control channel. The data transmission is done by the data channels. The control channel is known by all nodes and listens to them in no data to receive or to send.

The transceiver has a capability to switch to various channels such as data and control channels where each nodes has only one of this kind of transceiver.

For the ease of presentation and analysis, we use a circular transmission range R for each node if the distance is bigger than R then 2 nodes do not interfere. The acoustic signal has propagation speed which is v. And thus, the maximal propagation time T for the acoustic signal from a node to reach its transmission range equals R v . if the same channel when the signal for anode get received more than one node then packets get lost by collision.

Each node moves slowly or remains static and can able to notice their own position instruction. This is a reasonable assumption as localization has been widely explored for networks. Position information is needed by the functions of networking such as Geo-routing and environment monitoring applications. System cost will not increase in this assumption much. Though some localization strict synchronization is not needed where they need some synchronization service.

Each sensor is assumed to be able to communicate with the sink directly, which is reasonable because the average depth of the ocean is 4 km and the communication range of an acoustic signal can reach 10 km. Nevertheless, since the energy of a node is limited, it is better to communicate with neighboring nodes to reduce energy consumption.

Thus, multi-hop forwarding saves much energy consumption. Therefore, most of the communications in the paper are neighboring communication to reduce the energy consumption, even though the nodes can communication with the sink directly. That is why the slot size is assumed to the propagation delay between two neighboring nodes.

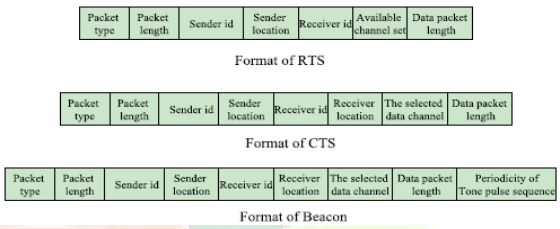


Fig. 3. Packet format of control messages

To increase the network applicability, the paper explores all kinds of communications, such as the sink-to-node, node-to-node, and node-to-sink communications.

III.ALGORITHM

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

The basic principle behind RSA is the observation that it is practical to find three very large positive integers e, d and n such that with modular exponentiation for all m: (m e) d ≡ m (mod n) {\displaystyle (m^{e})^{d}\equiv m{\pmod {n}}} {\ displaystyle (m^ {e})^{d} \equiv m{\pmod {n}}} and that even knowing e and n or even m it can be extremely difficult to find d.

Key Generation

The keys for the RSA algorithm are generated the following way:VChoose two distinct prime numbers p and q.

For security purposes, the integers p and q should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits'[2] to make factoring harder. Prime integers can be efficiently found using a primality test.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 10, March 2017

Compute n = pq.

n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

Compute $\lambda(n) = \text{lcm}(\lambda(p), \lambda(q)) = \text{lcm}(p - 1, q - 1)$, where λ is Carmichael's totient function. This value is kept private.

Choose an integer e such that $1 < e < \lambda(n)$ and $\gcd(e, \lambda(n)) = 1$; i.e., e and $\lambda(n)$ are coprime.

Determine d as $d \equiv e{-}1 \pmod{\lambda(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\lambda(n)$).

This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\lambda(n)}$.

e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 216 + 1 = 65,537. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.[13]

e is released as the public key exponent.

d is kept as the private key exponent.

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\lambda(n)$ must also be kept secret because they can be used to calculate d.

Alternatively, as in the original RSA paper,[2] the Euler totient function $\varphi(n) = (p - 1)(q - 1)$ can be used instead of $\lambda(n)$ for calculating the private exponent d. This works because $\varphi(n)$ is always divisible by $\lambda(n)$, and thus any d satisfying $d \cdot e \equiv 1 \pmod{\varphi(n)}$ also satisfies $d \cdot e \equiv 1 \pmod{\lambda(n)}$. However, computing d modulo $\varphi(n)$ will sometimes yield a result that is larger than necessary (i.e. $d > \lambda(n)$). Most RSA implementations will accept exponents generated using either method (if they use the private exponent d at all, rather than using the optimized decryption method based on the Chinese remainder theorem described below), but some standards like FIPS 186-4 may require that $d < \lambda(n)$. Any "oversized" private exponents not meeting that criterion may always be reduced modulo $\lambda(n)$ to obtain a smaller equivalent exponent.

Since any common factors of $(p - 1)$ and $(q - 1)$ are present in the factorisation of $n - 1 = pq - 1 = (p - 1)(q - 1) + (p - 1) + (q - 1)$,[14] it is recommended that $(p - 1)$ and $(q - 1)$ have only very small common factors, if any besides the necessary 2

IV.PROTOCOL DETAILS AND IMPLEMENTATION

In this section, to improve the channel utilization and to prevent the collisions for WSNs.

A. Slot Selection Constraints If a transmission pair has been scheduled in the network, the remaining slots cannot be used for transmission arbitrarily.

Free: this channel is free and can be used or reserved.

Reserved: here, some nodes have reserved for data packet transmissions.

Busy: this channel is busy in transmitting data packets.

The usage information of the data channel are been recorded in the table which is maintained by the node. Information such as locations, the destination node, source node, the length of its data packet and the channel status are been recorded in the table.

As a results, a slot can be classified into four sets, unable to transmit (UT), unable to receive (UR), unable both to transmit/receive (UB), and free both to transmit/receive (FB).

Performance comparison with Security

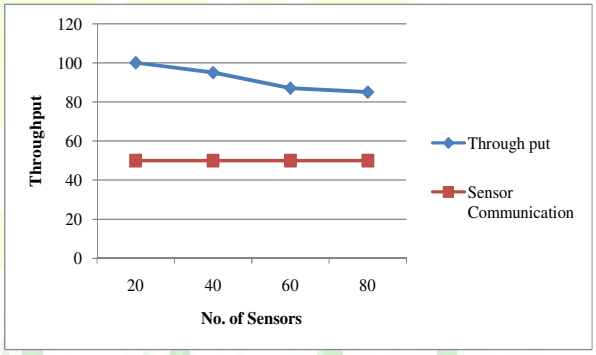


Fig. 5. Average Network Throughput

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 10, March 2017

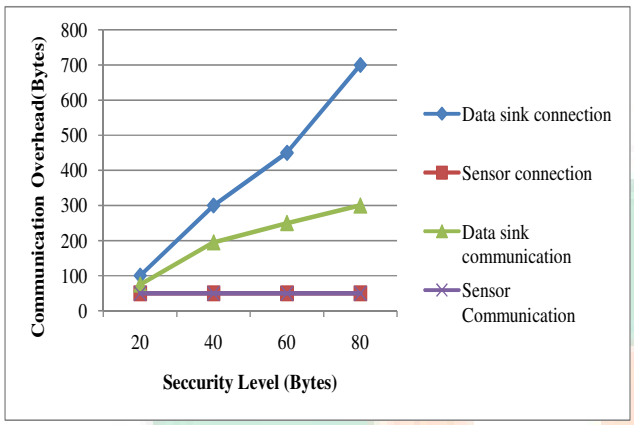


Fig.6. Security Levels & Over Head

V.CONCLUSION

The WSN communication is the most practical technology for real time entities. But the security is most preferable and needed one. Each and every data watched by a person or team to earn money with illegal operations of that hacked data. So Security is very essential one. This project is maintain the security in lightweight method. The efficiency of method is very high.

REFERENCES:

[1] Prosanta Gope, Tzonelih Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-time Application Data Access in Wireless Sensor Networks", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, 2016.

[2] I. F. Akyildiz, W. Su, Y. S. Subramaniam, E. Cayirci, "Survey on sensor network," IEEE Communication Magazine, vol.40, pp. 112-114, August 2002.

[3] O. Gnawali, K.-Y. Jang, J. Paek, M. Vieira, R. Govindan, B. Greenstein, A. Joki, D. Estrin, E. Kohler, "The tenet architecture for tiered sensor networks," in: Proc. SenSys 2006, ACM, pp. 153–166, October 2006.

[4] D. Yang, S. Misra, X. Fang, G. Xue, J. Zhang, "Two-tiered constrained relay node placement in wireless sensor networks: computational complexity and efficient approximations," IEEE Trans. Mobile Computing. vol. 11 no. 8 pp. 1399–1411, August 2012.

[5] P. Gope, T. Hwang, "BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network," IEEE Sensors Journal,Vol. 16 (5), pp. 1368 – 1376, March 2016.

[6] T. Nguyen, A. Al-Saffar, and E-N Huh, "A dynamic ID-based authentication scheme," Proceedings of the Sixth International Conference on Networked Computing and Advanced Information Management (NCM), pp. 248-253, August 2010.

[7] P. Gope, T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sensors Journal, vol. 15 (9), pp. 5340 – 5348, June 2015.

[8] K. H. M. Wong, Z. Yuan, C. Jiannong, and W. Sheng Wei, "A dynamic user authentication scheme for wireless sensor networks," in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp. 244-251, Taiwan, June, 2006.

[9] M.L. Das, "Two-factor user authentication in wireless sensor networks," IEEE Transaction on Wireless Communications. vol. 8 no. 3, pp. 1086–1090, March 2009.

[10] D. He, Y. Gao, S. Chan, C. Chen, J. Bu. "An enhanced two-factor user authentication scheme in wireless sensor networks," AdHoc & Sensor Wireless Networks vol. 10 no. 4, February 2010.

[11] H. Yeh, T. Chen, P. Liu, T. Kim, H. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," Sensors, vol. 11, no. 5 pp. 4767–4779, May 2011.

[12] R. Fan, D. He, X. Pan, L. Ping, "An efficient and dos-resistant user authentication scheme for two-tiered wireless sensor networks," Journal of Zhejinag Univ.-Science vol. 12 no.7 pp. 550–560, May 2011.

[13] D. Wang, P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle, and solutions," Computer Networks, vol. 73, pp. 41-57, November, 2014.

[14] P. Kumar, A.J. Choudhury, M. Sain, S.M. Lee, H.J. Lee, "RUASN: a robust user authentication framework for wireless sensor networks," Sensors, vol. 11 no. 5, pp.5020–5046, May 2011.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

[15] Q. Jiang, Z. Ma, J.F. Ma, G. Li, "Security enhancement of robust user authentication framework for wireless sensor networks," China Communication, vol. 9, no. 10, pp. 103–111, August 2012.

[16] TH Chen, WK. Shih, "A robust authentication protocol for wireless sensor networks," ETRI Journal, vol. 32, no. 5, pp. 704-712, October 2010.

[17] K. Xue, C. Ma, P. Hong, R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," Journal of Network Computer Applications, vol. 36 no. 1, pp. 316–323, January 2013.

[18] C. T. Li, C. Y. Weng, C. C. Lee, "An advanced temporal credential based security scheme with mutual authentication and key agreement for wireless sensor networks," Sensors, vol. 13, pp. 9589–9603, July 2013.

[19] A. K. Das, "A Secure and Efficient User Anonymity-Preserving Three- Factor Authentication Protocol for Large-Scale Distributed Wireless Sensor Networks," Wireless Personal Communications, vol. 82 no. 3: pp.1377-1404, January 2015.

[20] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," International Journal of Communication Systems DOI:10.1002/dac.2933, January 2015.

[21] Q. Jiang, J. Ma, X. Lu, Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," Peer-to-Peer Networking and Applications, June 2014.J. So and N. Vaidya, "Multi-Channel MAC for Ad Hoc Networks: Handling Multi-Channel Hidden Terminals Using a Single Transceiver," Proc. ACM MobiHoc, pp. 222-233, May 2004.

[22] J.S. Pathmasuntharam, A. Das, and A.K. Gupta, "Primary Channel Assignment Based MAC(PCAM)A Multi-Channel MAC Protocol for Multi-Hop Wireless Netwroks" Proc. IEEE Proc. Wireless Comm. and Networking Conf. (WCNC '04), pp. 1110-1115, 2004.

[23] S.-L. Wu, C.-Y. Lin, Y.-C. Tseng, and J.-P. Sheu, "A New Multi-Channel MAC Protocol with On-Demand Channel Assignment for Multi-Hop Mobile Ad Hoc Networks," Proc. Int'l Symp. Parallel Architectures, Algorithms, and Networks (I-SPAN '00), May 2000.

