ISSN: 0976-3104
SPECIAL ISSUE: (Emerging Technologies in Networking and Security (ETNS)

ARTICLE OPEN ACCESS

A SURVEY ON EFFICIENT CRYPTOGRAPHIC APPROACH FOR DATA SECURITY IN WIRELESS SENSOR NETWORKS

S. Ilakkiya*, M. Mailsamy, J. Gladson Maria Britto

Dept of Computer Science and Engineering, Vivekanandha College of Engineering for women, Namakkal, Tamilnadu, INDIA

ABSTRACT

Aim: A new symmetric encryption standard algorithm which is the amalgamation of two different encryption algorithms proposed by Nath et. Al namely TTJSA and DJSA algorithms in randomized method. The algorithm is named as Modern Encryption Standard version – I algorithm. The idea of modern encryption standard is to make a symmetric key cryptographic method which should be unbreakable. The MES version –I algorithm is effective against frequency analysis and spectral analysis. Further improvements can be bit level encryption can be performed on the text files after dividing the plaintext into two text files.

Published on: 2nd -December-2016

KEY WORDS

Keymanagement, WSN, random pre distribution

***Corresponding author:** **Email:** ilakskiya13081994@gmail.com; **Tel.:** +91 9944485920

INTRODUCTION

In modern digital communication era, allocation of information is collective significantly. The information being diffused is exposed to innumerable attacks. Therefore, the information security is solitary of the most challenging aspects of communication in any current network. This also smears to WSNs, specially those used in applications that monitor sensitive information (e.g., health care applications). These networks are quickly gaining popularity that they are potentially low cost solutions to a variety of real world challenges and are expected to play an essential role in the upcoming age of pervasive computing. However, the highly constrained nature of sensors imposes a difficult challenge: their reduced availability of memory, processing power and energy delays the deployment of many modern cryptographic algorithms considered safe.

Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not viable to be applied directly for wireless sensor networks. WSNs consist of tiny sensors which really ache from the deficiency of battery power, processing and memory. Any encryption scheme applying on WSNs require transmission of extra bits, hence extra processing, memory and battery power which are very central resources for the sensor's durability. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks [3]. There are some key queries arise when applying encryption schemes to WSNs like, how the keys are generated or dispersed. There is an important issue how the keys could be changed time to time for encryption as there is insignificant (or no) interaction for the sensors.There are other many issues how keys are revoked, assigned to a new sensor added to the network or rehabilitated for ensuring robust security for the network. There could not be an efficient solution for adopting of pre-loaded keys or embedded keys.

Data security

For this reason, the choice of the most memory, processing and energy efficient security solutions is of spirited importance in WSNs. To date, several dramatists have developed wide studies comparing different encryption algorithms. WSNs can be seen as a special type of ad-hoc network poised by a large number of little, low-cost and highly resource forced sensor nodes, known as spots. The sensors are spread in the area of interest, and can then meet and process data from the environment (e.g., mechanical, thermal, biological, chemical, and optical readings). They have applications in a variety of fields such as environment monitoring which involves checking look, dirt and marine, state based maintenance, habitat monitoring (determining the plant and animal species population and behaviour), seismic detection, military following, inventory chasing, smart spaces and rally sensing material in hostile locations, medical and home security to machine diagnosis, chemical/biological detection etc[6]. Spots are normally battery-powered, which has moved considerable research efforts on the development of energy mindful protocols, such as data link layer protocols. In general, one of the main goals driving the design of these systems is to improve network communications in order to save energy, and thus extend the network’s lifetime. On the other hand, security is regularly very forlornly considered at the very last step in the design of WSNs. Actually, most WSN organisations do not even consider security between their requirements because the effecting and energy outlays it adds to the system is seen as an adverse “extra cost” in such forced environments. However, in WSN-based applications that monitor sensitive information, it is vital to avoid eavesdropping, which is typically obtained by means of encryption systems (e.g., symmetric ciphers).Even when the evidence acquired is not confidential, it is still necessary to ensure data integrity and reality by means of message authentication mechanisms, since the approval of invalid data (generated either by natural causes or with malicious purposes) could lead to mistaken actions and severe values.

ARCHITECTURE

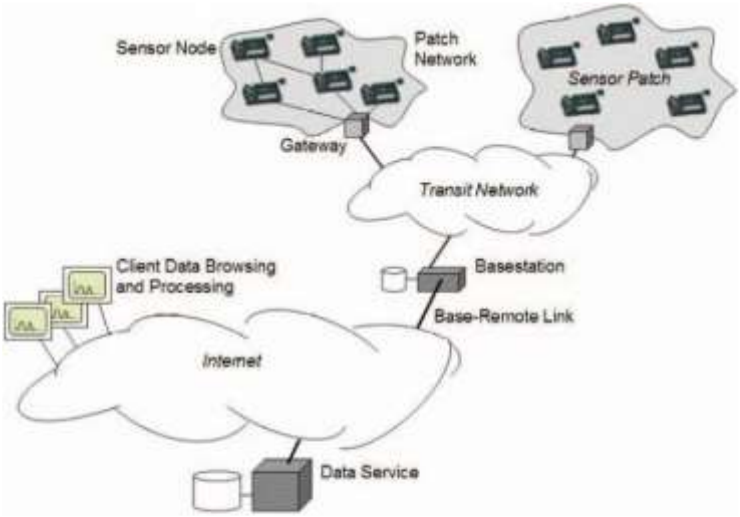

Fig: 1. Wireless sensor network

LITERATURE REVIEW

Key management deals with the secure generation, distribution, and Storage of keys. It plays a vital role in computer security today as practical attacks on public-key systems are typically aimed at key management as disparate to the cryptographic algorithms themselves.

In[1]Authors Abtin Keshavarzian, Elif Uysal-Biyikoglu in the paper” Energy-efficient Link Assessment in Wireless Sensor Networks “For energy on strained stationary wireless networks of sensom, selection of links with high quality rate helps to guarantee consistent long-term operation. During the implementation of a protocol aiming industrial applications of such systems, it was found that it is useful to acquire exact information about the availability and quality of the RF communication links prior to the network topology formation. “Link assessment" as part of the initialization process, undertakes this task by assessing a enough amount of packets exchanged between neighburing nodes. It introduces and analyze two different approaches to link valuation: The first attitude is a random nondeterministic scheme that permits for a probabilistic guarantee of collision-free packet exchange. An alternative method is described which employs 'ronstant-weight codes' and provides a determinklic guarantee 01 success [2]. In particular, a speciul class of constant-weight codes, known as optical orthogonal codes, are considered. Since, these codes are regularly permutable, they make the link assessment process simpler, and therefore they are preferred over other codes. And evaluate the performance of these methods based on their energy consumption, time duration, and implementation complexity.

In[2]Authors Theodoros Salonidis1, Pravin Bhagwat2, Leandros Tassiulas1, and Richard LaMaire3in the paper" Distributed Topology Construction of Bluetooth Personal Area Network" In recent years, wireless ad hoc networks have been a emergent area of research. While there has been considerable research on the topic of routing in such networks, the topic of topology creation has not received due devotion. This is since almost all ad hoc networks to date have been built on top of a single channel, broadcast based wireless media, such as 802.11 or IR LANs. For such networks the reserve relationship between the nodes obliquely (and uniquely) determines the topology of the ad hoc network. Bluetooth is a promising new wireless technology, which enables portable devices to form short-range wireless ad hoc networks and is built on a frequency hopping physical layer. This fact implies that hosts are not able to communicate unless they have previously discovered each other by matching their frequency leaping patterns. Thus, even if all nodes are within direct communication range of each other, only those nodes which are synchronized with the mast can get the transmission. To provision any-to-any communication, nodes must be synchronized so that the pairs of nodes (which can communicate with each other) together form a connected graph. Using Bluetooth as an example, this rag first provides deeper insights into the issue to link establishment in frequency hopping wireless systems [6]. It then announces the Bluetooth Topology Costruction Protocol (BTCP), an asynchronous distributed protocol for constructing scatternets which starts with nodes that have no knowledge of their surroundings and sacks with the formation of a connected network satisfying all connectivity constraints posed by the Bluetooth technology [6]. To the best of our knowledge, the work presented in this paper is the first attempt at building Bluetooth scatternets using distributed logic and is quite "practical" in the sense that it can be implemented using the communication primitives offered by the Bluetooth 1.0 specifications.

In[3]Authors Elyes Ben Hamida, Guillaume Chelius in the paper"Revisiting Neighbor Discovery with Interferences Consideration" In wireless multi-hop networks, hello protocols for neighbor finding are a basic overhaul existing by the networking hoard. However, their study usually rely on quite simplistic models which do not take into version problems ensuing from low level layers, such as the physical layer. One of the individualities of radio communications is the presence of interferences which decrease the size of the medium. A random hello protocol inspired by aloha and study the impact of the interferences on the neighbordiscovery process[7]. As expected, and prove that, in average and in the presence of interferences, a node discovers only a subset of its neighbours and analytical model to compute the average number of nodes that a given node may expect to discover in its neighborhood. Finally,can present a hello protocol with sleep periods and show how to optimize this protocol using our hybrid model. A real scenario stemming from the CAPNET project is then analyzed and studied.

In[4]Authors Sudarshan Vasudevan, Jim Kurose, Don Towsley presented in the paper"On Neighbor Discovery in Wireless Networks With Directional Antennas" The problem of neighbour discovery in static wireless ad hoc networks with directional antennas. Then propose several probabilistic processes in which nodes perform random, independent shows to discover their one-hop neighbors. Our neighbor sighting algorithms are confidential into two sets, viz. Direct- Discovery Procedures in which nodes discover their neighbors only upon receiving a transmission from their neighbors and Gossip-Based Algorithms in which nodes gossip about their neighbors' location evidence to allow faster discovery. consider the operation of these algorithms in a fit, synchronous system and mathematically derive their optimal parameter settings. How to cover these algorithms for an asynchronous system and describe their optimal design. Analysis and simulation of the algorithms show that nodes discover their neighbors much sooner using conversation-created processes than using through-discovery algorithms. Furthermore, the routine of gossip-based algorithms is insensitive to an surge in node density. The efficiency of a neighbor discovery algorithm also depends on the choice of antenna beamwidth. How the choice of beamwidth effects the performance of the finding process and provide insights into how nodes can construct their beamwidths.

In [5] Authors Jason Hill and David Culler {jhill, culler}@cs.berkeley.edu presented in the paper“ A wireless embedded sensor architecture for system-level optimization” Power consumption and abilities of the radio statement layer are the prevailing factors in total system concert. It presents a wireless sensor node architecture to achieve high communication bandwidth with the bounce to efficiently implement novel communication protocols. The architecture is instantiated in an operational design using viable microcontroller and radio technology. Its ability to adjust system act by using unusual protocols is by four case studies involving power management, synchronization, localization, and wake-up.

In[6] Authors N. B. Anuar, M. L. M. Kiah, V. A. Rohani,D. Petkovi presented in the paper” Key management protocol with end-to-end data security and key revocation for a multi-BS wireless sensor network”, A significant wireless device network with several base stations (BS), a key management protocol is planned in it. For confidently conveying data between a node and a base station or two nodes, an end-to-end data security method is accepted by this protocol. Further using a distributed key reversal scheme to efficiently remove conceded nodes then forms our key management protocol celled multi-BS key management protocol (MKMP).

In [7] Authors W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh presented in the paper “BHNFDIA Energy Efficient Elimination of Black Hole and False Data Injection Attacks in Wireless Sensor Networks “The trustworthy containers will be accelerated and malicious packets will be unwanted nearly. The proposed scheme can exclude false data injection by outside malicious nodes and Black hole attack by compromised insider nodes. Replication results show that the scheme can successfully identify and eliminate 100% black hole nodes. Malicious packets are immediately impassive with 100% filtering efficiency. The pattern ensures more than 99% packet delivery with better network traffic.

In [8] Authors D. H. Yum and P. J. Lee presented in the paper”Hands-On Experiences in Deploying Cost-Effective Ambient-Assisted Living Systems “The prototype is built upon inexpensive, off-the-shelf hardware (e.g., various sensors, Arduino microcontrollers, ZigBee-attuned wireless communication modules) and license-free software, there by warranting low system deployment costs. The network embraces nodes placed in a house’s main rooms or mounted on furniture, one wearable node, one actuator node and a centralized processing element (coordinator). Upon detecting significant abnormalities from the conventional movement patterns of individuals and/or sudden falls, the system issues automated alarms which may be forwarded to legal care patrons via a variety of statement channels.

In [9] Authors F. Gandino, B. Montrucchio, and M. Rebaudengo presented in the paper “Information Assurance Based on Cryptographic Checksum with Clustering Security Management Protocol “To swear information security beside security attacks and particularly node seizing attacks and propose a cluster security management protocol, called Cryptographic Checksum Clustering Security Management (C3SM), to offer an competent reorganised security management for hierarchal networks. In C3SM, every cluster selects dynamically and alternately a node as a cluster security manager (CSM) which issues a episodic shared secrete key for all nodes in the cluster.

In [10] Authors W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili presented in the paper” Hybrid Intelligent Routing in Wireless Mesh Networks: Soft Computing Based Approaches “Wireless Lattice Networks (WMNs) are the evolutionary identity-forming multi-hop wireless networks to ability last mile access. Due to the rise of stochastically varying network environments, steering in WMNs is disapprovingly affected. This Integrated Link Cost (ILC) is added for each link based upon throughput, delay, jitter of the link and remaining energy of the node and is used to calculate shortest path between a given source-terminal node pair.

COMPARISION OF DIFFERENT TECHNIQUE

By Comparing these keys to rally the protocols for proficiency for energy consumption can be highly accomplished. And expense of an increased node density and network latency.

Table I

S.NO	TITLE OF THE PAPER	KEYS/PROTOCOLS	SECURITY	DEMERITS
	Energy efficient	RandomKey Distribution	Energy Efficient	Require Large Recall

[1]	Link Assessment in Wireless Sensor Networks			Space To Store The Ring.
[2]	Distributed Topology Construction of Bluetooth Personal Area Network	Bluetooth Topology construction protocol	Short-range radio link between movable devices	The Topology certainly affects its operation and performance
[3]	Revisiting Neighbor Discovery with Interferences Consideration	Hello protocol	A Symmetric link neighbor will include your id in its neighbor list.	Larger Hello message size in dense networks.
[4]	On Neighbor Discovery in Wireless Networks With Directional Antennas	Neighbor discovery Algorithm	Efficient in tracking the nodes with in a node's communication range.	Static and dynamic multihop Sensor Networks.Conventional node discovery techniques were found to be inadequate and they give less significance to the QoS parameters.
[5]	A wireless embedded sensor architecture for system-level optimization	Multi BS Management protocol	Additional load on router equipment	It may affect the stability of the other protocols.
[6]	Key management protocol with end-to-end data security and key revocation for a multi-BS wireless sensor network	Key Management Protocol	It deals with the secure generation, distribution and storage of keys.	Difficult to check Routing information.
[7]	BHNFDIA Energy Efficient Elimination of Black Hole and False Data Injection Attacks in Wireless Sensor Networks	Black hole and false data injection	Simple form of Selective forwarding attack, where a malicious node may drop all the packet passing through it without forwarding to the sink node.	Malicious Node Communicates the Destination Node with false route information.
[8]	Hands-On Experiences in Deploying Cost Effective AmbienAssisted Living Systems	Plain Global Key Scheme	Modification	The System Administrator stores this information in the memory of the nodes.
[9]	Information Assurance Based on Cryptographic Checksum with Clustering Security Management Protocol	cluster security management protocol	Increase the Energy Consumption of Sensor Nodes, Strong Resilience Against Node Capture With Lower Key Storage.	An Enemy That knows the master key and the identification number of the cluster head can extract the cluster key and easily Attack the cluster.

[10]	Hybrid Intelligent Routing in Wireless Mesh Networks: Soft Computing Based Approaches	Transistor Key	Fabrication, modification	False information to the neighboring nodes, packet loss, selective forwarding attack

S

SIBLE SOLUTION

The main benefit of q-s-composite is represented by an efficient memory management, which allows to store a larger quantity of keys and consequently it can improve the resilience of the protocol. This result is reached by means of a new key generation mechanism and by limiting the quantity of starting keys per link.

CONCLUSION

The potential drawbacks of the proposed scheme have been analyzed and an in-depth analysis has shown that their effects are overcome by the security improvements. A comparison with state-of-the-art schemes shows that the proposed approach represents the best solution for large mobile WSNs, and that it is also the best solution for static WSNs, if the nodes can be compromised during the initialization phase.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Seo SH, Won J, Sultana S, Bertino E. [2015] Effective key management in dynamic wireless sensor networks, Information Forensics and Security, IEEE Transactions on. 10(2):371–383.

[2] Gisbert J, Palau C, Uriarte M, et al. [2014] Integrated system for control and monitoring industrial wireless networks for labor risk prevention, Journal of Network and Computer Applications. 39:233–252.

[3] Hackmann G, Guo W, Yan G, et al. [2014] Cyber physical co design of distributed structural health monitoring with wireless sensor networks, Parallel and Distributed Systems, IEEE Transactions on. 25(1):63–72.

[4] Rezaee AA, Yaghmaee MH, Rahmani M,et al. [2014] Hoca: Healthcare aware optimized congestion avoidance and control protocol for wireless sensor networks, Journal of Network and Computer Applications. 37:216–228.

[5] Moosavi H, Bui F. [2014] A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks, Information Forensics and Security, IEEE Transactions on. 9(9):1367–1379.

[6] Shamshirband S, Anuar NB, et al. [2014] Co-fais: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks, Journal of Network and Computer Applications. 42(0):102–117.

[7] Bechkit W, Challal Y, Bouabdallah A,Tarokh V. [2013] A highly scalable key pre-distribution scheme for wireless sensor networks, Wireless Communications, IEEE Transactions on. 12(2):948–959.

[8] Dai H, Min Zhu Z, Gu XF. [2013] Multi-target indoor localization and tracking on video monitoring system in a wireless sensor network, Journal of Network and Computer Applications. 36(1):228–234.

[9] Das AK. [2012] Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks. IJ Network Security. 14(1):1–21.

[10] Yum DH, Lee PJ. [2012] Exact formulae for resilience in random key pre distribution schemes, Wireless Communications, IEEE Transactions on. 11(5):1638–1642.

[11] Gandino F, Montrucchio B, Rebaudengo M. [2014] Key management for static wireless sensor networks with node adding, Industrial Informatics, IEEE Transactions on. 10(2):1133–1143.

[12] Blom R. [1985] An optimal class of symmetric key generation systems, in EUROCRYPT 84 workshop on Advances in cryptology: theory and application of

cryptographic techniques. New York, NY, USA:Springer-Verlag. 335–338.

[13] Du W, Deng J, Han YS, Varshney PK, Katz J, Khalili A. [2005] A pairwise key predistribution scheme for wireless sensor networks, ACM Trans. Inf. Syst. Secur.8(2)228–258.

[14] Xiao Y, Rayi VK, Sun B, Du X, Hu F, Galloway M. [2007] Asurvey of key management schemes in wireless sensor networks, Computer Communications. 30:11-12,2314–2341.

[15] Madhusudhanan B, Chitra S, Rajan C. [2015] Mobility Based Key Management Technique for Multicast Security in Mobile Ad Hoc Networks, The Scientific World Journal, Hindawi Publishing Corporation.

[16] Bechkit W, Challal Y, Bouabdallah A, Tarokh V. [2013] A highly scalable key pre-distribution scheme for wireless sensor networks, Wireless Communications, IEEE Transactions on. 12(2):948–959.

[17] Das AK. [2012] A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks, International Journal of Information Security. 11(3):189–211.

[18] Zhu S, et al. [2006] Leap+: Efficient security mechanisms for large scale distributed sensor networks, ACM Transactions on Sensor Networks. 2(4):500–528.

[19] Gandino F, Montrucchio B, Rebaudengo M. [2014] Key management for static wireless sensor networks with node adding, Industrial Informatics, IEEE Transactions on. 10(2):1133–1143.