International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

Volume 5 Issue 2 July - December 2015

International Manuscript ID : 22308849072015-02

EFFECTIVE ALGORITHM FOR SECURITY AND INTEGRITY IN WIRELESS SENSOR NETWORKS

Aayushi
Assistant Professor
Computer Science and Engineering
M.M.E.C, Mullana
Ambala Haryana, India

Reeta Devi
Assistant Professor
Computer Science and Engineering
S. P. C. E. T.
Lalru, Mohali, Punjab, India

ABSTRACT

Security is one of the major and key concerns in the network communications from long ago. A number of algorithms are developed so far by enormous researchers and practitioners, still this domain is having huge scope of research as the cracking and hacking attempts are increasing in assorted networks. In this manuscript, an effective and unique algorithm is proposed for the security and integrity in wireless sensor networks that makes use of dynamic hash key. This approach can be used in WSN as well as cloud environment. The proposed approach is making use of hybrid algorithm including IPSec protocol in which the hash techniques are used. The results in the proposed algorithm are giving effective and optimal results.

Keywords - Network Security, WSN Security, Cloud Security

INTRODUCTION

Wireless communication [1] is becoming more popular among the users now a days and this is mainly due to the technological revolution in the field of mobile phones, laptops, PDA, wireless LAN and modems. It provides communication among a network of disconnected users; these users may be mobile or stationary. The use of wireless technology has become a ubiquitous method to access the Internet or connect to the local network whether in a corporate, educational, or private setting. Practically all laptop computers are currently sold with a built-in wireless adapter. In handheld units like PDAs, wireless adapters have also become standard and are now being introduced in some types of mobile phones. It is much easier and inexpensive to deploy a wireless network compared to a traditional wired network, as the required effort and cost of running cables are negligible. Furthermore, additional devices can be added to the network at no extra cost.

In order for a wireless equipped device to access other computers on the wireless local network [2] or connect to the Internet it must associate with a wireless access point. A wireless access point is a device that allows devices equipped with wireless adapters to be linked together in a local area network [3] and to connect to a pre-existing wired LAN and via a gateway to get access to the Internet. Such networks are called wireless local area networks (WLANs) as the wireless access point is linking wireless devices without wires. Because of the convenience of not having to rely on wires, WLANs have become immensely popular. When devices equipped with wireless adapters are part of a WLAN and are managed by a wireless access point, their coordination is controlled by a centralized entity. The devices rely on the presence of a fixed infrastructure, i.e., wireless access points to work. Laptop computers must be within the range of a wireless access point to connect to other devices because the laptops must communicate via the access point.

There are two different approaches to establish the communication among a number of hosts. The first approach is to use an existing cellular hierarchy which carries data as well as voice; in the cellular network, there is a centralized administration or a fixed base station which handles routing and resource management procedures, since all the routing decisions are made in a centralized manner. Therefore these networks are also called Infrastructural based networks. But the main problem here is handoff between two areas when user moves from one cell to other. It becomes an important to transfer data without any delay while handoff. Another main problem is that it is limited to the area where network is present. In the second approach we can form an ad hoc network among all users who wants to communicate with each other. This means all the users in the ad hoc network [9] must be willing to forward data packets to make sure that the packets are delivered from the source to destination. This form of networking is smaller than the cellular approach and only limited in the range by the individual nodes transmission range. This system has its own advantages over cellular system and these are on demand setup, Fault tolerance and unconstrained connectivity [15].

REVIEW OF LITERATURE

To propose and defend the research work, a number of research papers are analyzed. Following are the excerpts from the different research work performed by number of academicians and researchers.

Rong Du et. al. (2014) [4] - In this paper, the work considers the problem of building a secure network against node conspiracy attack that based on network segmentation. As we know, network coding has demonstrated its great application prospects in wireless sensor network (WSN) transmission. At the same time, it is facing a variety of security threats, especially conspiracy attack. In existing research, secure coding design strategies are much more than secure topological structure. In this work, a secure scheme is proposed from the perspective of topology and network segmentation. Based on the network segmentation and topology design, the network coding transmission is weakly. In this paper, the work investigated the topology design and network segmentation issue for weakly secure against node conspiracy attack. We analyzed how the network segmentation and topology design influenced the security of networks. This paper proposed a secure strategy against node conspiracy attack by network segmentation and topology design. This work compared the ISTD and ISNS strategies. Simulations showed that the proposed routing algorithm ISNS achieved good performance. It can cope with larger structures and more malicious node network than ISTD. As a future research, we will study the secure topology design strategy under a large number of malicious nodes and a larger structure.

Chris Karlof (2003) [5] - This manuscript considers and process the routing security in wireless sensor networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. This work propose security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks—sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. This paper describes crippling attacks against all of them and suggest countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks.

David Wagner (2004) [6] – This paper introduce TinySec, the first fully-implemented link layer security architecture for wireless sensor networks. In our design, we leverage recent lessons learned from design vulnerabilities in security protocols for other wireless networks such as 802.11b and GSM. Conventional security protocols tend to be conservative in their security guarantees, typically adding 16--32 bytes of overhead. With small memories, weak processors, limited energy, and 30 byte packets, sensor networks cannot afford this luxury. TinySec addresses these extreme resource constraints with careful design; we explore the tradeoffs among different cryptographic primitives and use the inherent sensor network limitations to our advantage when choosing parameters to find a sweet spot for security, packet overhead, and resource requirements. TinySec is portable to a variety of hardware and radio platforms. The experimental results on a 36 node distributed sensor network application clearly demonstrate that software based link layer protocols are feasible and efficient, adding less than 10% energy, latency, and bandwidth overhead.

Wenliang Du (2004) [7] - To achieve security in wireless sensor networks, it is important to be able to encrypt messages sent among sensor nodes. Keys for encryption purposes must he agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial. Many key agreement schemes used in general networks, such as Diffie-Hellman [10] and public-key based schemes, are not suitable for wireless sensor networks. Pre-distribution of secret keys [14] for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. Recently, a random key pre-distribution scheme and its improvements have been proposed. A common assumption made by these random key pre-distribution schemes is that no deployment knowledge is available. Noticing that in many practical scenarios, certain deployment knowledge may be available a priori, we propose a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. This work show that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can he substantially improved with the use of our proposed scheme. The scheme and its detailed performance evaluation are presented in this paper.

Jun Zhao (2014) [8] - The seminal q-composite key predistribution scheme is used prevalently for secure communications in large-scale wireless sensor networks. Yagan and this work explore topological properties of WSNs employing the q-composite scheme in the case of q = 1 with unreliable communication links modeled as independent on/off channels. However, it is challenging to derive results for general q under such on/off channel model. In this paper, the work resolve such challenge and investigate topological properties related to node degree in WSNs operating under the q-composite scheme and the on/off channel model. Our results apply to general q, yet there has not been any work in the literature reporting the corresponding results even for q = 1, which are stronger than those about node degree. Specifically, we show that the number of nodes with an arbitrary degree asymptotically converges to a Poisson distribution, present the asymptotic probability distribution for the minimum node degree of the network, and establish the asymptotically exact probability for the property that the minimum node degree is at least an arbitrary value. Numerical experiments confirm the validity our analytical findings.

PROBLEM FORMULATION AND THE PROPOSED WORK

In a static Network, nodes may fail for several reasons and the network may split into two or more disconnected partitions. This may deteriorate or even nullify the usefulness and effectiveness of the network. Therefore, repairing partitions is a priority. In this paper we present a method to repair network partitions by using mobile nodes. By reasoning upon the degree of connectivity with neighbors, a mobile node finds the proper position where to stop in order to reestablish connectivity. Factors influencing the method performance are singled out and criteria for their selection are discussed. Simulations show that the proposed method is effective and efficient not withstanding packet loss. The existing approaches of using secured and trusted protocols for any kind of network infrastructure. The IPSec protocols are needed in almost every network infrastructure to keep the data channel and transmission secured.

PROBLEM IN EXISTING SYSTEM

The classical approach is not security and integrity efficient in terms of the implementation to any network scenario. In the specialized cases of static Network, the nodes may crash for assorted reasons. The network may split into two or more disconnected partitions. The classical approach deteriorates or damage or even nullify the usefulness and effectiveness of the network. For these reasons, repairing partitions is a priority. The classical approach can be improved and enhanced to repair network partitions by using mobile nodes. By reasoning upon the degree of connectivity with neighbors, a mobile node finds the proper position where to stop in order to reestablish connectivity. Factors influencing the method performance are singled out and criteria for their selection are discussed. Using simulated environment, the proposed method can be proved efficient and effective not withstanding packet loss.

The advantages of the IPSec [11, 12] includes Access control Connectionless integrity Data origin authentication, Rejection of replayed packets, A form of partial sequence integrity Confidentiality (encryption) In a firewall/router provides strong security to all, Traffic crossing the perimeter, Resistant to bypass. Below transport layer, hence transparent to Applications, to be transparent to end users can provide security for individual users if desired

ADVANTAGES OF THE PROPOSED SYSTEM

- The proposed system is generating efficient results in terms of the optimal solution when executed using IPSec.
- The proposed technique is efficient also in terms of the Jitter and Throughput despite of the number of iterations
- The limitations may be included regarding the proposed work in terms of its further enhancement using assorted metaheuristics.
- The proposed system may give better results in executed using simulated annealing that is one of the prominent metaheuristic techniques

PLATFORM AND TOOLS USED FOR IMPLEMENTATION

1. ns2 [13]

2. xgraph
3. gnuplot
4. Red Hat Linux
5. sed
6. awk

RESULTS AND ANALYSIS

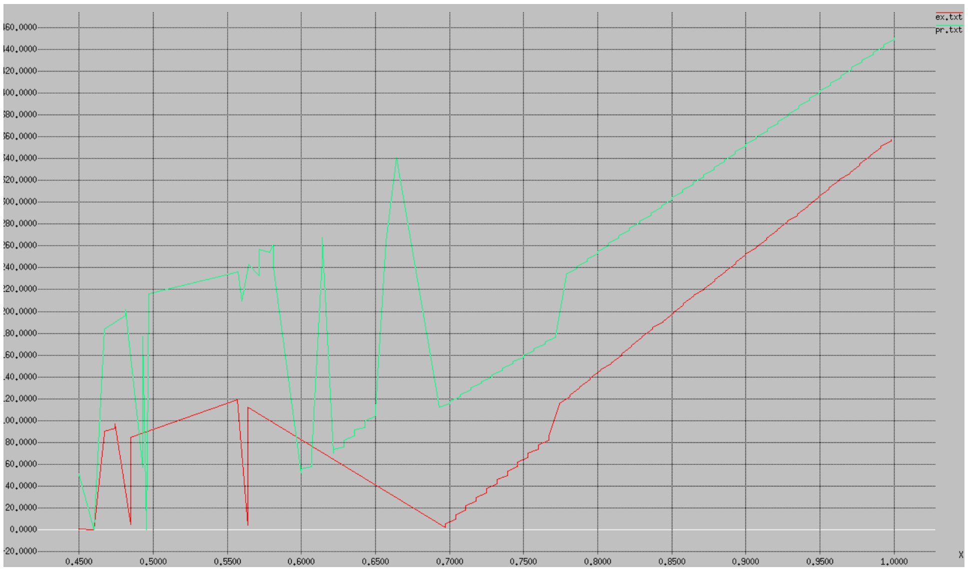

Figure 1 – The Data Transmission Rate in Existing and Proposed Techniques

The efficiency of the network entirely depends on the data transmission rate in the channels. It is evident from Figure 1 that the data transmission rate the classical approach is very less than the proposed approach.

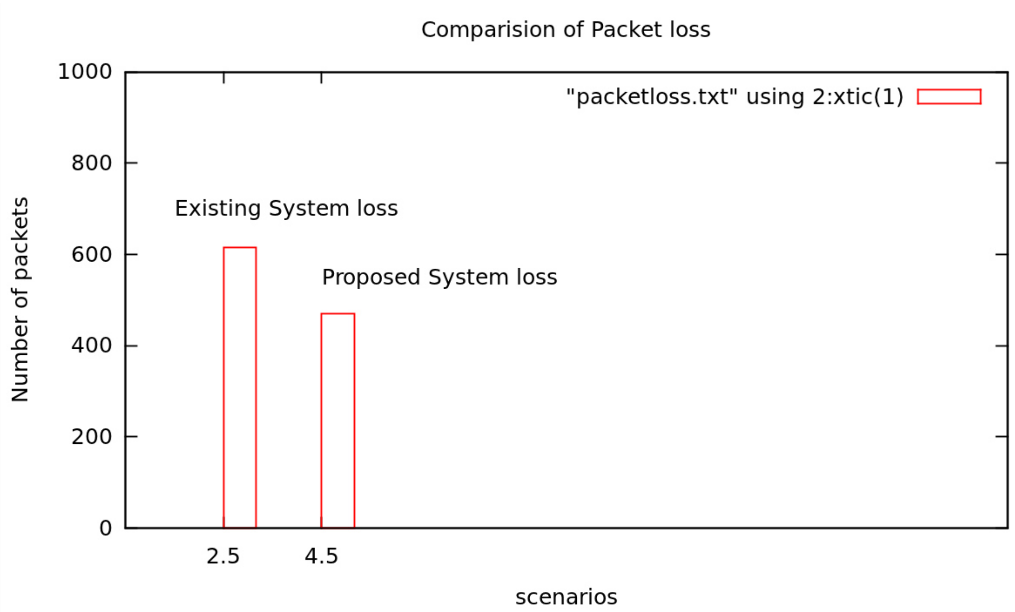

Figure 2 – Comparative Analysis of Packet Loss Rate in Existing and Proposed Approach

The higher packets loss in the network transmission cause huge delay and turnaround time. The proposed approach is providing very less packet loss by which the overall effectiveness of the system is improved.

Existing Approach - Efficiency	**Proposed Approach – Efficiency**
60	85

Existing Approach - Jitter	**Proposed Approach - Jitter**
20	16

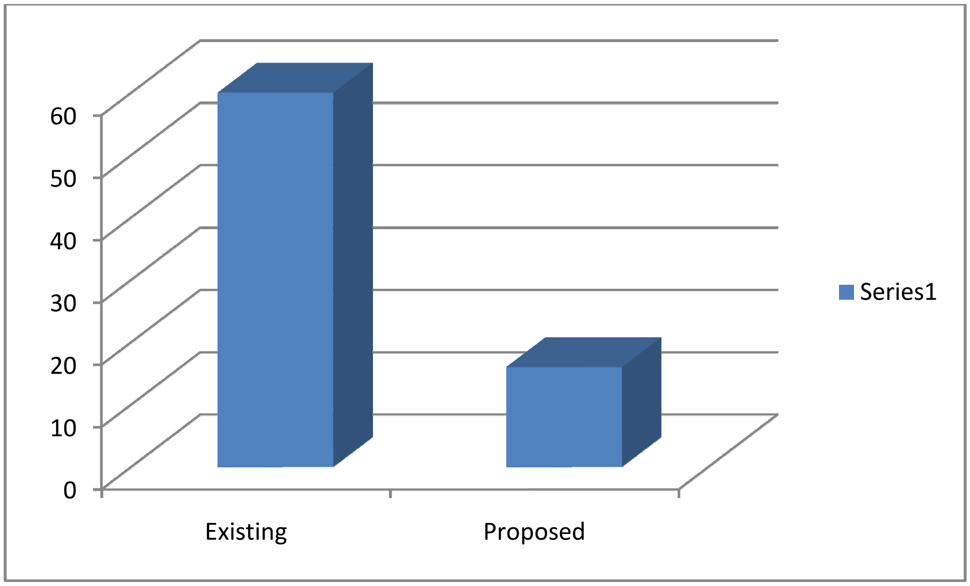

Figure 3 – Comparative Analysis of Jitter in Existing and Proposed Approach

The jitter parameter is one of the important aspects in the wireless network transmission which can damage the entire communication. The proposed approach is having very less jitter as compared to the classical approach by which the integrity of the system is improved.

CONCLUSION AND SCOPE OF FUTURE WORK

An assorted stack of protocols and techniques are used for accomplishing the task of security and privacy in WSNs. But the proposed work is implemented with a unique set of tasks and steps. There are number parameters or metrics which are required be considered for the integration and analysis of security aspects. Remote or basically remote sensor framework or wireless sensor network having different and spread independent and also optional sensors to screen physical or natural conditions, for instance, temperature, sound, weight, et cetera and to supportively go their data through the framework to a guideline territory. The all the more front line frameworks are bi-directional, in like manner enabling control of sensor activity. The change of remote sensor frameworks was convinced by military applications, for instance, battle zone observation; today such frameworks are used as a piece of various present day and buyer applications, for instance, mechanical technique checking and control, machine wellbeing watching, and so forth. In this examination work, the ID of noxious center the extent that the bundles got to in separated. For future scope of the work, the metaheuristic and parallel approaches can be used in hybrid approach to better and efficient results.

REFERENCES

[1] Rev, A. H. (2003). Wireless sensor networks.

[2] Crow, B. P., Widjaja, I., Kim, J. G., & Sakai, P. T. (1997). IEEE 802.11 wireless local area networks. Communications Magazine, IEEE, 35(9), 116-126.

[3] Fowler, H. J., & Leland, W. E. (1991). Local area network characteristics, with implications for broadband network congestion management. Selected Areas in Communications, IEEE Journal on, 9(7), 1139-1149.

[4] Du, R., Zhao, C., Li, S., & Li, J. (2014). Efficient weakly secure network coding scheme against node conspiracy attack based on network segmentation. EURASIP Journal on Wireless Communications and Networking, 2014(1), 1-9.

[5] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.

[6] Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, 47(6), 53-57.

[7] Du, W., Deng, J., Han, Y. S., Chen, S., & Varshney, P. K. (2004, March). A key management scheme for wireless sensor networks using deployment knowledge. In INFOCOM 2004. Twenty-third AnnualJoint conference of the IEEE computer and communications societies (Vol. 1). IEEE.

[8] Yavuz, F., Zhao, J., Yagan, O., & Gligor, V. (2014, June). On secure and reliable communications in wireless sensor networks: Towards k-connectivity under a random pairwise key predistribution scheme. In Information Theory (ISIT), 2014 IEEE International Symposium on (pp. 2381-2385). IEEE.

[9] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y. C., & Jetcheva, J. (1998, October). A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking (pp. 85-97). ACM.

[10] Joux, A. (2000). A one round protocol for tripartite Diffie–Hellman. In Algorithmic number theory (pp. 385-393). Springer Berlin Heidelberg.

[11] Ferguson, N., & Schneier, B. (2000). A cryptographic evaluation of IPsec. Counterpane Internet Security, Inc, 3031.

[12] Elkeelany, O., Matalgah, M. M., Sheikh, K. P., Thaker, M., Chaudhry, G., Medhi, D., & Qaddour, J. (2002). Performance analysis of IPSec protocol: encryption and authentication. In Communications, 2002. ICC 2002. IEEE International Conference on (Vol. 2, pp. 1164-1168). IEEE.

[13] Issariyakul, T., & Hossain, E. (2011). Introduction to network simulator NS2. Springer Science & Business Media.

[14] Hwang, J., & Kim, Y. (2004, October). Revisiting random key pre-distribution schemes for wireless sensor networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (pp. 43-52). ACM.

[15] Gupta, G., & Younis, M. (2003, March). Fault-tolerant clustering of wireless sensor networks. In Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE (Vol. 3, pp. 1579-1584). IEEE.