IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Robust, secure and Optimized Shortest Acknowledge based Multi-packet Reception for Wireless Networks

P.meenakshi *1, Mr.G.Bhanu Prasad*2

[1]M.Tech Student, Department of CSE, Mallareddy Engineering College For Women, Dulapally, Kompally, Secunderabad, Telangana state, India, meenakshi6meena@gmail.com.

[2]Associate Professor, Department of CSE, Mallareddy Engineering College For Women, Dulapally, Kompally, Secunderabad, Telangana state, India, bhanu.gorantla2020@gmail.com.

ABSTRACT

In the era of the Information Technology world, w here Internet plays the important role in mentioning the whole world as the global village. In that aspect Communication medium is the back bone of the system. In the medium of the wireless sensors network where data flows form a source if hub through he routing protocol mechanism is the most important. In this paper, we try to put forward the concept of the Cryptographic key management for the managing the secure data transmission. Extending the support of the protocol where the encryption and decryption methodology plays to give the transmission. We have taken consideration of the access control based approach where data sharing would base on the group based specific and acknowledgment based approach to implement the best cryptographic approach. In order to secure the best of the privacy we have implemented the dynamic group based encryption and decryption mechanism the key fact behind this paper is try give the extension to the classical mechanism where the optimization is not up to the mark of satisfaction. Here we consider the each and every node and its associated hub to attach to the parent node which we maintain the security sand optimization in the map reduced programming.

KEYWORDS: Delay-tolerant routing; packet delivery delay distribution; communication cost distribution, Wireless networks, ad hoc networks, multipacket reception, network management, neighbor discovery.

I.INTRODUCTION

Early developments in wireless sensor networks were motivated by military applications, which have the highest security requirements among the various applications of WSNs . Military sensing networks are designed to detect and gain as much information as possible about enemy movements, explosions, and other phenomena. Typically, wireless sensor nodes are integrated with military command,

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. Examples of military wireless sensor network applications include battlefield surveillance, guidance systems for intelligent missiles, detection of attacks by weapons of mass destruction such as nuclear, biological, or chemical weapons and other monitoring applications.

Fig.1.1. Illustration of the WSN

Key management protocols for WSNs should support the underlying network layer by providing easy mechanisms to support this dynamic nature. Our proposed protocol provides complete support for adaptive cluster-based networks.

II.RELATED WORK

Environmental monitoring can vary from indoor to outdoor monitoring. In a large building, sensor nodes can be set up to monitor light, temperature, status of frames (windows, doors), air streams and indoor air pollution. Additionally, WSNs can be used for reducing the impact of fire and earthquake damages. A fire and smoke detector system integrated with light signals indicating exits can be built to help guide the trapped residents through the safest route and save their lives. In another scenario, earthquake damage can be measured by incorporating wireless sensors inside cement blocks during construction, or their attachment to structural units. Inspecting a building after an earthquake using such a system will not only facilitate evaluation of cracks and damages, but will also provide real data for modeling and prediction of structural damages to the building in future events.

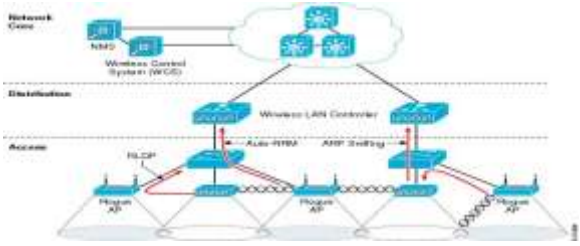

Fig.2.1. Model View of the Node Based WSN

In the split-phase model, the consumer of an interface signals a request for a particular service. The provider of the interface is then responsible for performing the service, and signaling an event to the consumer when the service has completed. Programmatically, in order for these operations to be non-blocking, Tiny OS introduces the concept of tasks, which are code segments that are scheduled to run at a later time. Tasks are

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

put in a run-to-completion, first-come, first-serve queue. In essence, one component calls a command on another component.

III.PROPOSED METHODOLOGY

WSNs have a wide variety of applications in agriculture. The applications in this category are mainly focused on enhancing the efficiency and growth of cultivations. For example, WSNs are used in a vineyard to monitor temperature of grapes and to perform survey of the micro climate. It turns out that the network was not only helpful for the farmers, but every participant in the wine making process, from the time of growing the grapes to wine production and marketing, benefited from it. A similar system is also used for controlling the water usage in an efficient and economic way by monitoring moisture in soil, air humidity and weather forecasting. Other goals of this system include frost detection and warning as well as pesticide application and disease detection. In general, crop management, Industries can take most benefit out of WSNs. The industrial WSN global survey 2012 stated that 70% of the industrial users are planning WSNs or additional deployments within the next 18 months. Some of the important sectors of industry where WSNs can benefit include factory automation, process control, real-time monitoring of the health of the machinery, detection of liquid/gas leakage, remote monitoring of contaminated areas, and real-time inventory management, etc. In one interesting application, British Petroleum (BP) used WSNs to improve safety and product quality by monitoring warehouses and storage management of barrels. The concept is that motes attached to barrels will be capable of locating nearby objects, detecting their content and alerting in case of incompatibility (danger of a chemical reaction), aging effects of the enclosure, etc. Similar to BP, other oil companies installed sensors to measure temperature in their pipeline sys terms. Besides, the communication in WSNs is done via the wireless medium, which is inherently insecure and invariably incurs various types of security threats. Many attacks such as denial of service, replay, fabrication, hello flood, wormhole, etc., which are common in other wireless networks (i.e., mobile ad hoc network (MANET), wireless fidelity (WiFi), etc.) are also applicable to WSNs. However, many well-known security mechanisms devised for other wireless networks cannot be applied directly to the resource limited WSNs because of the architectural disparity of the networks. Furthermore, a majority of sensor networks are deployed in hostile environments with presence of intelligent adversaries. Hence, security is critical for the practical deployment of WSNs. In the next subsections, we describe the major security challenges in WSNs.

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

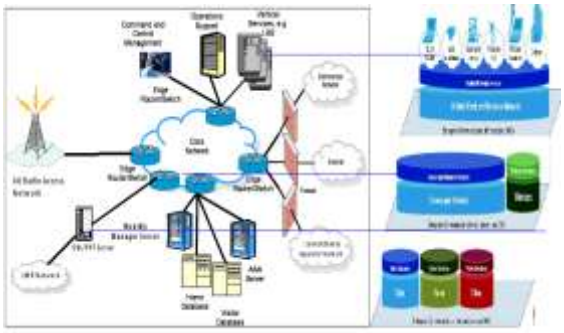

Fig.3.1. Architecture Model of the WSN in the context View

When two member nodes from different clusters want to communicate with each other, they need to establish a secure path via some KM nodes. Let us assume that node i from one cluster wants to communicate with node j in another cluster. In such a scenario, node i performs the following steps:

i. Node i find a KM node in its own cluster and send an encrypted message to that KM node.

ii. The KM node then sends the message to another KM node belonging to the cluster of node j using the procedure.

iii. Finally, the KM node of node j sends the encrypted message to node j using the same procedure.

A key management protocol is not complete if it does not provide mechanisms for revocation and key refresh. Given indefinite time, any network can be compromised if it does not refresh the key periodically. In addition, it is necessary to revoke the key of the compromised node once identified to continue with normal network operation. In our scheme, the base station is responsible for revoking the keys of the compromised nodes. We assume that with the help of intrusion detection systems, such as , the compromised nodes can be detected and a list, R composed of the IDs of compromised nodes is sent to the base station.

IV.EVALUATION AND ANALYSIS

Unlike traditional wireless networks, sensors are expected to be deployed arbitrarily in an enemy territory (in military reconnaissance scenarios) or over dangerous or hazardous areas. In this setup, an adversary can easily capture the physical mote (which is essentially a node in the sensor network. In this paper, we use mote and node interchangeably.) And read sensitive information such as cryptographic keys stored in the internal memory. In addition, the adversary can take control of and manage the mote remotely, which makes it further difficult to detect physical tampering. Even if the base station resides in a friendly or safe area, the sensor nodes need to be protected from being compromised. Therefore, protocols should have built in mechanisms to limit the damage in the event of node capture and other physical attacks.

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

V.CONCLUSION AND FUTURE WORK

Securing and authenticating the communication between the nodes in a WSN is very challenging, especially because the nodes are typically deployed unattended, often in conditions unfavorable to human monitoring and lacks a mechanism for secure storage for cryptographic keys, which make them vulnerable to many attacks. Moreover, these tiny sensor nodes are limited in power, computation, memory and bandwidth, which make it harder to implement other existing security infrastructure such as public key cryptography. Therefore, in WSNs, it is necessary for the communicating parties to share encryption keys before a secure communication can take place. This necessitates the use of robust key management protocols that handle the task of distributing, establishing and managing keys between sensor nodes.

VI.REFERENCES

[1] A. Doria, M. Uden, and D. P. Pandey, Providing connectivity to the saaminomadic community, in Proceedings of the 2nd International Conference onOpen Collaborative Design for Sustainable Innovation (dyd 02), Bangalore, India, Dec 2002.

[2] A. Pentland, R. Fletcher, and A. A. Hasson, A road to universal broadband connectivity, in Proceedings of the 2nd International Conference on Open Collaborative Design for Sustainable Innovation (dyd 02), Bangalore, India, Dec 2002.

[3] G. E. Prescott, S. A. Smith, and K. Moe, Realtime information system technology challenges for NASAs earth science enterprise, in Proceedings of The 20th IEEE RealTime Systems Symposium, Phoenix, Arizona, Dec 1999.

[4] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, Energyefficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet, in Proceedings of ACM ASPLOS, 2002.

[5] Disruption tolerant networking, http://www.darpa.mil/ato/solicit/DTN/.

[6] J. Ott and D. Kutscher, A disconnectiontolerant transport for drivethruinternet environments, in Proceedings of IEEE INFOCOM, 2005.

[7] G. W. Boehlert, D. P. Costa, D. E. Crocker, P. Green, T. OBrien, S. Levitus, and B. J. Le Boeuf, Autonomous pinniped environmental samplers; using instrumented animals as oceanographic data collectors, Journal of Atmospheric and Oceanic Technology, vol. 18, no. 11, pp. 18821893, 2001, 18 (11).

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

[8] T. Small and Z. Haas, The shared wireless infostation model a new ad hoc networking paradigm (or where there is a whale, there is a way), in Proceedings of The Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003), June 2003, pp. 233244.

[9] K. Fall, A DelayTolerant Network Architecture for Challenged Internets, SIGCOMM, August 2003.

[10] A. Beaufour, M. Leopold, and P. Bonnet, Smarttag based data dissemination, in First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA02), June 2002.

[11] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry, Epidemic algorithms for replicated database maintenance, in Proceedings of the ACM Symposium on Principles of Distributed Computing, 1987, pp. 112.

[12] W. Vogels, R. V. Renesse, and K. Birman, The power of epidemics: Robust communication for largescale distributed systems, In Proceedings of HotNetsI'02: First Workshop on Hot Topics in Networks, special issue of the ACMSIGCOMM Computer Communication Review, Princeton, NJ. October 2002.

[13] Delay tolerant networking research group, http://www.dtnrg.org.

[14] P. Zhang, C. M. Sadler, S. A. Lyon, and M. Martonosi, Hardware design experiences in zebranet, In Proc. ACM SenSys, pages 227238, 2004.

[15] M. Motani, V. Srinivasan, and P. Nuggehalli, PeopleNet: Engineering a Wireless Virtual Social Network, In Proc. ACM Mobicom, pages 243257, Aug. 2005.

[16] J. Partan, J. Kurose, and B. N. Levine, A Survey of Practical Issues in Underwater Networks, In Proc. ACM WUWNet, pages 1724, Sept. 2006.

[17] A. Maffei, K. Fall, and D. Chayes, Ocean Instrument Internet, In Proc. AGU Ocean Sciences Conf., Feb 2006.