International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

AN DISTRIBUTED REPROGRAMMING PROTOCOL IN WIRELESS SENSOR NETWORKS

M.Dhanalakshmi, G.Gayathri

M.E (Cse) Scholar, Varuvan Vadivelan Institue Of Technology
Assistant Professor, Varuvan Vadivelan Institue Of Technology

***Abstract*--In MWSN, security is one of the main constrain for transmission of data in network, in existing system arises drawback in security area of WSN. We implement the protocol named secure distributed reprogramming protocol (SDRP) for efficient transaction; it has limited bandwidth support of data (1.6Ghz) transmission in network. It also suitable only for homogenous network, SDRP is implemented in centralized approach. In this approach, involve of base station they reprogram the alternate path for sending data to destination in the period of false node arises in the network. In centralized approach, if base station fails the sensor nodes lose the connection to the base station and it is not possible to carry out the reprogramming in the network. To enhanced the security for wireless sensor network by using reprogramming in the network for data transmission. In reprogramming the alternate path can be scheduled in the time of any intruder occurrences in the network for data transmission.**

Keywords: MWSN, secure distributed reprogramming protocol (SDRP), Reprogramming

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The envisaged size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust, although functioning 'motes' of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

Survey

Er. Balihar Singh, Er. VarinderjitKaur,"A Modified Approach for Aggreration Technique in WSN" Vol. 5(6), 2014.A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year.Sensors are hardware devices that produce measurable response to a change in a physical condition like temperature and pressure. Sensors sense or measure physical data of the area to be monitored the continual analogsignal sensed by the sensors is digitized by an Analog-to-digital converter and sent to controllers for further processing.

B.Sudhakar and K.Sangeetha,"Multi Sink based Data Collection Scheme for Wireless Sensor Networks"Vol.2, Special Issue 1, March 2014.Characteristics and requirements of Sensor node should be small size, consume extremely low energy, operate in high volumetric densities, be autonomous and operate unattended, and be adaptive to the environment. As wireless sensor nodes are micro-electronic sensor device, can only be equipped with a limited power source of less than 0.5 Ah and 1.2 V. Sensors are classified into three categories. Passive, Omni Directional Sensors: Passive sensors sense the data without actually manipulating the environment by active probing. They are self-powered i.e energy is needed only to amplify their analog signal. There is no notion of "direction" involved in these measurements. Passive, narrow-beam sensors: These sensors are passive but they have well-defined notion of direction of measurement. Typical example is 'camera'.

Active Sensors: These groups of sensors actively probe the environment, for example, a sonar or radar sensor or some type of seismic sensor, which generate shock waves by small explosions. The overall theoretical work on WSN's considers Passive, Omni directional sensors. Each sensor node has a certain area of coverage for which it can reliably and accurately report the particular quantity that it is observing. Several sources of power consumption in sensors are a) Signal sampling and conversion of physical signals to electrical ones, b) signal conditioning, and c) analog-to-digital conversion. Spatial density of sensor nodes in the field may be as high as 20 nodes/ m3.

Ambika.N andG.T.Raju"Linear Programming Model of Sensor Network"Vol. 5 (2) , 2014, To enhanced the security in, wireless sensor network, by using of reprogramming in the network for data transmission. In reprogramming the alternate path can be scheduled in the time of any intruder occurrences in the network for data transmission. Using zero knowledge protocol and single sign mechanism provides security in data transmission. The protocol have unlimited amount of bandwidth for data transmission to destination.

The single sign mechanism provides high verification of user in the network. The performance of trade off analysis of energy consumption and Quality of Services gain in reliability and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. To urbanized a novel probability model for analyze the best redundancy level in terms of path redundancy (mp) and source redundancy (ms), as well as the best intrusion recognition settings in terms of the number of voters (m) and the intrusion incantation interval under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes.

Finally, our analysis results to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes to prolong the system lifetime. For future work, to explore more extensive malicious attacks in addition to packet dropping and each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks.

Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture certain strategic nodes with higher probability, alternate between benign and malicious behaviour and collude with other attackers to avoid intrusion detection. To investigate the use of trust/reputation management to strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbour nodes, as well as to tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs. In situations where concurrent query traffic is heavy, we plan to explore trust-based admission control to optimize application performance.

Objective

In centralized approach, if base station fails the sensor nodes lose the connection to the base station and it is not possible to carry out the reprogramming in the network. By using reprogramming in the network for data transmission to enhanced the security for wireless sensor network. In the time of any intruder occurrences in the network for data transmission for reprogramming the alternate path can be scheduled.

Architecture For Resistance to Node and User Compromised Attacks

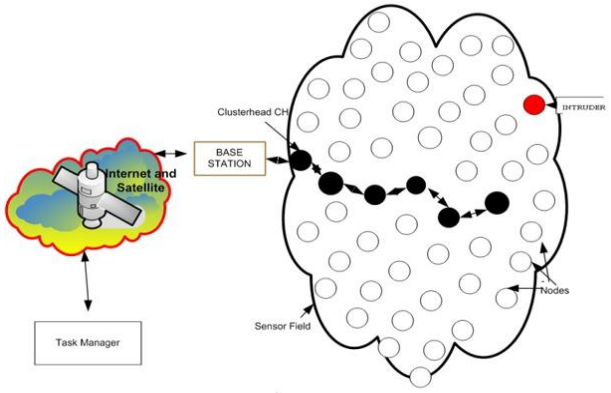

Fig. 1.1 Architecture

II. RELATED WORK

We are unacquainted of the earlier technique of Automatic test packet generation[1]from the performance and requirements to transfer the information between the sender and receiver[7]. The ATPG is used to send the packet to check the network whether it has the faulty links[8] and then the packet will clear the problem [5] through the data plane with the help of anteater [2] [6]. A NICE way of open flow application is used to reduce the identified bugs and KLEE technique is used to automatically generate the test packets and find the similar differences between the tools used in the complex system programs [3] [4].The closest related article we know is the Quantum cryptography.

Quantum cryptography technique is used to transfer the information from the sender to receiver in a secure way by means of quantum key distribution. The QKD is used to generate the polarised photon that is used to transmit the digital information. The polarization technique is used in this cryptography to find out the eavesdropper intercept into the communication and the photon destroys the process of eavesdropper and therefore the interrupter can be found out.

In the earlier technique of ATPG(Automatic Test Packet Generation), it cannot be able to model the boxes because the test packets will change the internal state and the failed rule can take a backup rule active and hence the information can be hacked in easy way.

The quantum key cryptography consists of the protocols, They are BB84, decoy state protocol, E91 protocol, SARG04, DPS protocol, S09 protocol, S13 protocol. These protocols are used to exchange the quantum information (qubit). The two quantum mechanical system is used to produce the polarization of a single photon. Vertical polarization or Horizontal polarization is used as a two states in the quantum computing.

The operation of a pure qubit is quantum logic state and standard basic measurement Quantum logic state is used to transfer the information as a unitary transformation and standard basic measurement is used to gain the state of the information.

AES(Advanced Encryption Standard) is used in this quantum key cryptography to transfer the information securely without hacking by the third party. AES is used as a substitution and permutation network. AES has the block

size of 128 bits and the size of key is 128,192 or 256 bits. AES calculation was done in finite fields. It operates on 4X4 matrix to transfer the information from the plain text to the cipher text.

AES algorithm: This algorithm has high-level description such as KeyExpansion, InitialRound (AddRoundKey), Rounds (SubBytes, ShiftRows, Mixcolumns, AddRoundKey) and Final Round (SubBytes, ShiftRows, AddRoundKey).

The strength of AES algorithm is that it able to protect the shared information up and around the secret level. The key length used in the TOP SECRET information is either 192 or 256 bits and the performance of the AES algorithm is high, It requires low RAM and a wide variety of hardware is used from 8-bit smart cards to the high-performance computers and hence the AES technique is used in the Quantum Cryptography to share the information.

III. PROPOSED SCHEME

A new quantum cryptography scheme has claimed its security by providing well-organized security arguments.

The intermediate nodes along the path to the sink are able to verify the authenticity and integrity of the incoming packets using a predicted value of the key generated by the sender's cybernetic energy, thus requiring no need for specific rekeying messages.

AES(Advanced Encryption Standard) is able to efficiently detect and filter false data injected into the network by malicious outsiders.

The performance of the quantum key cryptography is high and the time taken to transfer the information to the receiver is low.

REFERENCES

[1] Hongyi Zeng, Member, IEEE, Peyman Kazemian, Member, IEEE, George Varghese, Member, IEEE, Fellow, ACM and Nick McKeown, Fellow, IEEE, ACM,"Automatic Test Packet Generation," in IEEE/ACM TRANSACTIONS ON NETWORKING,vol.22,NO.2,APRIL 2014.

[2] H. Mai, A. Khurshid, R. Agarwal, M. Caesar, P. B. Godfrey, and S. T.King, "Debugging the data plane with Anteater," *Comput.Commun.Rev., vol. 41, no. 4, pp. 290–301, Aug. 2011.*

[3] M. Canini,D.Venzano, P. Peresini,D.Kostic, and J. Rexford, "A NICEway to test OpenFlow applications," in *Proc. NSDI, 2012, pp. 10–10.*

[4] C. Cadar, D. Dunbar, and D. Engler, "Klee: Unassisted andautomatic generation of high-coverage tests for complex systemsprograms," in *Proc. OSDI, Berkeley, CA, USA, 2008, pp. 209–224.*

[5] A. Dhamdhere, R. Teixeira, C. Dovrolis, and C. Diot,"Netdiagnoser:Troubleshooting network unreachabilities using end-to-end probes and routing data," in *Proc. ACM CoNEXT*, 2007, pp. 18:1–18:12.

[6] N. Duffield, F. L. Presti, V. Paxson, and D. Towsley, "Inferring linkloss using striped unicast probes," in *Proc. IEEE INFOCOM*, 2001,vol. 2, pp. 915–923.

[7]N. Duffield, "Network tomography of binary network performance characteristics," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp.5373–5388, Dec. 2006.

[8] Y. Bejerano and R. Rastogi, "Robust monitoring of link delays andfaults in IP networks," *IEEE/ACM Trans. Netw.*, vol. 14, no. 5, pp.1092–1103, Oct. 2006.