INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 6, Issue 1 JAN 2017

Reducing Replication Attacks by Implementing Security Framework in Wireless Sensor Networks

[1]KAMMA. RAMU,[2]U. PRASAD

[1]B. Tech Student, Department of CSE, Nalanda Institute of Engineering & Technology, Village SiddharthNagar, Kantepudi, Mandal Sattenapalli, District Guntur, Andhra Pradesh, India.

[2]Assistant Professor, Department of CSE, Nalanda Institute of Engineering & Technology, Village SiddharthNagar, Kantepudi, Mandal Sattenapalli, District Guntur, Andhra Pradesh, India.

ABSTRACT─ ***Wireless Sensor Networks (WSN) are a field of research that has more than a few functions both for mass public and military. A wireless sensor network is composed of many sensors which can be utilized to monitor physical or environmental stipulations, reminiscent of temperature, sound, and pressure. After collecting this information they will have to pass this information through the network to an important region. A Sensor Node in wireless Sensor community lacks resources equivalent to processing potential, memory capability, battery energy, and communication potential. Because of the confined assets on sensor nodes, using traditional key management procedures in wireless sensor networks is confined. Key establishment is the predominant cryptographic primitive in all varieties of applications the place protection is a challenge. Authentication and pair wise key institution are crucial in sensor networks. In this paper, we furnish a survey of key management schemes in wireless sensor networks. Through our proposed system, we can decrease the replication attacks without reducing the network performance.***

1. INTRODUCTION

A wireless sensor community (WSN) consists of spatially dispensed autonomous sensors. These sensors are used to watch bodily or environmental stipulations, such as temperature, sound, stress, and so on. To cooperatively pass their knowledge via the community to a major place, the more brand new networks are bi-directional which makes it possible for manipulate of sensor recreation. The industrial and purchaser functions, reminiscent of industrial process monitoring and control, desktop health monitoring. There is a lot of advancement related to the network oriented strategy of the wireless based scenario on the basis of the ad hoc relative aspect in a well oriented fashion by the implementation of the mobile communication oriented analysis with an effective transmission of the data in the form of the packets in 3 - tier strategy. However, in sensor networks that make use of the existing key pre distribution approaches for pair wise key establishment as well as authentication between sensor nodes and mobile sinks, the Employment of mobile sinks for data collection elevates a new security challenge. In this paper, we proposed a common three-tier security framework for authentication as well as pair wise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-

based key pre distribution approach significantly improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre distribution approach. With two separate key pools as well as having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink. Here a strategy of the 3 - tier based scenario in which network oriented with respect to the ad hoc based scenario where there is an accurate implementation of the system based strategy in a well efficient manner are faced problems related to the mobility of the nodes based aspect in a well respective fashion respectively. Here this particular strategy takes place in the scenario of the networks of the large scale oriented fashion respectively. Here a new technique is proposed by the powerful aspect of the implementation based strategy in a well effective manner by the protocol oriented with the routing of the opportunistic strategy in a well desired fashion based on the efficient position based scenario in a well analyzed respective fashion in order to overcome the problems of the several previous methods in a well respective strategy. Here this particular system is implemented by the help of the property oriented with stateless fashion by the implementation of the scenario related to the aspect of the broad cast of the routing based geographic strategy in a well effective manner takes place in the system in a well oriented aspect respectively.

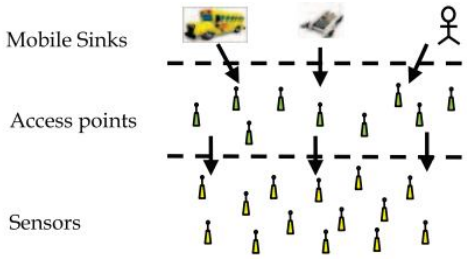
2. RELATED WORK

With the intention to exchange knowledge securely in WSN, the keys need to be shared among the nodes. Eschenauer and Gilgor proposed a probabilistic key pre-distribution which is the basic Scheme. The important thought was once to randomly opt for a set of keys from a key pool by way of a sensor node and any two nodes competent to find at the least one common key can use that key as their shared secret to provoke verbal exchange. Chan et al increased the elemental scheme and developed two key pre distribution schemes: the q-composite key pre-distribution scheme and the random pair sensible keys scheme. Q composite key pre distribution scheme requires at the least q customary keys with the intention to have a communique link between any two nodes.

Zhu et.al., described that LEAP (Localized Encryption And Authentication Protocol), a key administration protocol for sensor network that's designed to aid in network processing. This method can be used for assisting more than a few conversation models. The fundamental rationale of this scheme is that they may be able to provide authentication, confidentiality and robustness. Amar Rasheed et.al., proposed a scheme which uses polynomial pool based key pre distribution alongside the probabilistic key pre distribution scheme to set up a pair smart key between mobile sink and any sensor node. This scheme guarantees that the sensor node can establish a pair smart key with a cellular sink with high likelihood and without sacrificing safety. A. Rasheed et.al. also described a key distribution scheme which is based on random key pre distribution for heterogeneous sensor network that can achieve higher performance and security as in comparison with homogenous community. The proposed scheme reduces the storage requirements by using making use of iteration keys.

3. FRAMEWORK

A. System Architecture



In this network there are three different tiers. One for sink node, one for access points and another for sensor nodes; every tier contains a key pool with set of keys and these keys will be exchanged at the time of transmission of data.

The stationary access point proven at above act as authentication entry aspects to the network for triggering the sensor nodes to transmit their knowledge to the mobile sinks device. Mobile sink gadget sends data request message to the sensor nodes via stationary access point. Information request messages from the cellular sink device to stationary entry node to triggering sensor nodes of community, which transmit requested data to cell sink. Safety framework mostly uses two separate polynomial key pools as the cellular polynomial pool and the static polynomial pool. Polynomials from cell polynomial pool are used to set up authentication between cell sinks and stationary entry point which permit cellular sinks to access the network for data gathering. Polynomial from static pool is used to set up authentication and key setup between sensor nodes and stationary access point.

B. Methodology

In this paper a method is designed with a powerful strategy in which it is implemented for the accurate analysis based strategy followed by the improvement in the performance respectively. Here the implementation of the present method is shown in the figure and is explained in the elaborative fashion respectively. Here the present method completely overcomes the drawbacks of the several previous methods in a well efficient fashion respectively. There is a huge challenge for the present method in which the designed framework is to be efficient where there is an accurate analysis with respect to the implementation of the aspect that is problems of the previous methods in a well oriented fashion respectively then after there is an improvement in the degradation of the performance in the previous method where there is an overall improvement in the system based aspect with respect to the entire outcome respectively.

Key Pre-distribution:

A mobile polynomial pool of size |M| as well as a static polynomial pool of size |S| is created. To reduce the mobile polynomial compromise when the stationary access nodes are captured, the number of polynomials within the cellular sink must be more than the quantity of polynomials in every stationary entry node. So all cellular sinks and stationary access nodes are randomly given Km and one polynomial (Km>1) from M. By the way, all the sensor nodes and the stationary access nodes choose a subset of Ks and Ks-1 polynomials from S.

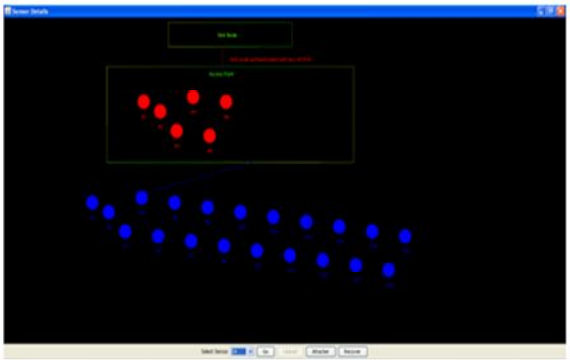
Key discovery and path establishment:

In initial stage, we expect that there aren't any assaults throughout deployment. After the key pre-distribution, key discovery as well as course among the nodes needs to be based. For a cell sink V to acquire information from a sensor node U, there should be an authentication course between cellular

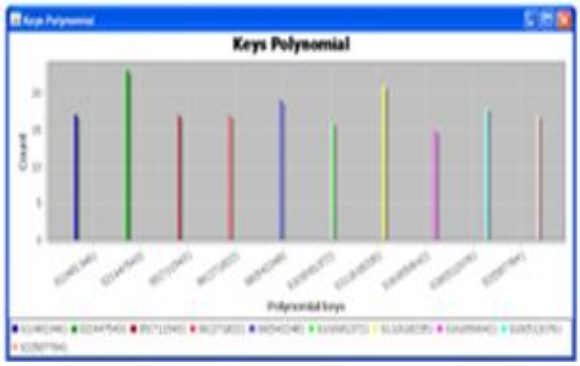
sink V and sensor node U by means of a stationary node A.

4. EXPERIMENTAL RESULTS

In this be taught, we've chosen the Blundo scheme to construct our approach. As we shall see, the Blundo scheme provides a transparent security assurance. Use of the Blundo scheme, thus, broadly eases the presentation of our study and permits us to furnish a clearer security evaluation. In the proposed scheme, we use two separate polynomial pools: the Mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial pool are used to set up the authentication between cellular sinks and stationary access nodes, so that you can permit these mobile sinks to access the sensor network for knowledge gathering. As a consequence, an attacker ought to compromise at least a single polynomial from the cellular pool to acquire access to the network for the sensor's information gathering. Polynomials from the static polynomial pool are used to determine the authentication and keys setup between the sensor nodes and stationary entry nodes.



The above screen describes that the authentication process & data transmission in three tier network.



The above screen describes that the graphical representation of the present method respectively. The above graph represents what the polynomial key count (number of keys) is taken by each sensor node.

5. CONCLUSION

In this paper a method is designed with a well efficient framework for the effective analysis followed by the improvement in the security based strategy followed by the entire system based outcome in a well oriented fashion respectively. In this paper, we proposed a general three-tier security framework for authentication and pair wise key establishment between mobile sinks as well as sensor nodes. We have further enhanced the security performance of the proposed scheme against stationary access node replication attack by strengthening the authentication mechanism between stationary access nodes as well as sensor nodes. We utilized the one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme.

REFERENCES

[1] J. L. X. Li, M. R. Lyu, "Taodv: A trusted aodv routing protocol for mobile ad hoc networks," in Proceedings of Aerospace Conference, 2004.

[2] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, and L. Besson, "Design and implementation of a trust-aware routing protocol for large wsns," International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 3, Jul. 2010.

[3] A. Rezgui and M. Eltoweissy, "Tarp: A trust-aware routing protocol for sensor-actuator networks," in IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007), 8-11 2007.

[4] 2 A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," Comput. Commun., vol. 30, pp. 2826– 2841, October 2007.

[5] S. Chang, S. Shieh, W. Lin, and C. Hsieh, "An efficient broadcast authentication scheme in wireless sensor networks," in Proceedings of the 2006 ACM Symposium on Information, computer and communi- cations security (ASIACCS '06). New York, NY, USA: ACM, 2006, pp. 311–320.

[6] K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 6, no. 11, pp. 4136 –4144, november 2007.

[7] P. De, Y. Liu, and S. K. Das, "Modeling node compromise spread in wireless sensor networks using epidemic theory," in World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006. International Symposium on a, 2006, pp. 7 pp. –243.

[8] A. Woo, T. Tong, and D. Culler, "Taming the underlying challenges of reliable multihop routing in sensor networks," in Pro- ceedings of the First ACM SenSys'03, Nov. 2003.

[9] S. Ganeriwal, L. Balzano, and M. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sen. Netw., 2008.