ENHANCING SECURITY FOR WIRELESS SENSOR NETWORK USING CRYPTOGRAPHY: A DIFFIE-HELLMAN ALGORITHM APPROACH

***Amandeep Kalra & **Dr. S. S. Khurmi**
*Assistant Professor, Deptt. of Computer Science and Engineering, Gulzar Group of Institutes, Khanna, Ludhiana
**Professor, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi Sabo

Abstract

For a secure and con dential network, wireless sensor networks need to ensure a dedicated crypt algorithm path to be deployed. Certain metrics ensure that the deployed crypt algorithm are fruitful for sending as well as receiving con dential message packets. Mobile ad-hoc network are wireless networks which leads to on-demand network creation and destruction, when no more in use. This every time new network can lead to malicious traps and loss of message packets. Authors have studied and analysed wireless sensor networks to recover the network from this loop and proposed a new algorithm for the same. Metrics discussed in the paper are deployed over the proposed algorithm to propose an ef cient network.

Keywords: [Wireless Sensor Networks (WSN), Dif e-Hellman algorithm, RSA algorithm, Routing Algorithms, Cryptography]

Introduction

Wireless networking is a technology which enables two or more computers to communicate within certain set of proposed protocols. The main feature of wireless network is that there exists no network cabling. Many wireless solutions for business as well as institutions applications are shaped with the emergence of standards such as IEEE 802.11, which is cost effective and easy to install. Wireless networks are helpful in case of handheld devices as well as warehousing, where installation of wired network is near to impossible.

A Wireless Sensor Network (WSN) is a type of wireless ad-hoc network that deploys a large number of low-cost sensor devices distributed over an area of interest. Collaboratively, they report sensor readings to a data collection sink or Base Station (BS), regularly or based on demand. The potential uses of this network range from military to civil applications. (Rahayu, 2015)

Benefits of Wireless Network

Mobile Ad- Hoc Network due to its infrastructure-less (no definite structure) structure and node mobility possess following advantages:

i. Fast installation
ii. Dynamic topologies
iii. Fault tolerance
iv. Connectivity
v. Mobility
vi. Cost
vii. Spectrum reuse possibility

Sensor networks are being deployed for a wide variety of applications, including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments etc. The trusted server scheme depends on a trusted server for key agreement between nodes, e.g., Kerberos. This type of scheme is not suitable for sensor networks because there is usually no trusted infrastructure in sensor networks.

There is need to either distribute public keys into nodes through the base station online, which may cause high communication overhead or pre distribute public keys into nodes offline, which may need some scheme to improve its efficiency. Such key exchange constraints lead to the loss of security in the network transmissions. So, in order to achieve a secured network, choosing of the appropriate key requires a lot of labor and wise decision. On the type of protocols deployed, the key used may vary according to the need and type of message or documents communicated.

There is need to either distribute public keys into nodes through the base station online, which may cause high communication overhead or pre distribute public keys into nodes offline, which may need some scheme to improve its efficiency. Such key exchange constraints lead to the loss of security in the network transmissions. So, in order to achieve a secured network, choosing of the appropriate key requires a lot of labor and wise decision. On the type of protocols deployed, the key used may vary according to

the need and type of message or documents communicated.

Literature Survey

In this section, various research works will be studied that have contributed to bring out a new ray of research in Wireless Sensor Networks as well as Cryptography.

With the smooth drift in technology from Wired Networks to Wireless Networks, new opportunities and challenges fascinated researchers in this field. Wireless Sensor Networks eased the path of mobility and computation in a network. This section deals with research contributions in Wireless Sensor Networks field.

There is need to either distribute public keys into nodes through the base station online, which may cause high communication overhead or pre distribute public keys into nodes offline, which may need some scheme to improve its efficiency. Such key exchange constraints lead to the loss of security in the network transmissions. So, in order to achieve a secured network, choosing of the appropriate key requires a lot of labor and wise decision. On the type of protocols deployed, the key used may vary according to the need and type of message or documents communicated.

Akkaya and Younis (2003) presented advances in wireless sensor networks where energy awareness was an essential consideration, that have led to several new protocols exclusively designed for sensor networks. Specific attention has been drawn onto the routing protocols since they might differ depending on the application and network architecture.

Kurmi et al (2017) focussed on WSN which carry maximum number of Sensor Nodes (SNs) that transfers the data from one system to another system without making use of any wires. The Lifetime of this network is Limited because all these SNs in the network are resource constraint. So, various researchers allowed numerous approaches for maximize the lifetime of the WSNs.

Merhi et al (2012) presented paper on security frameworks of wireless sensor network localization application that can no longer be ignored. Wireless sensor network are being deployed in sensitive environment that require high levels of confidentiality, integrity and authenticity.

Lal (2017) focussed on Network security for protecting data and message from cybercrime. Symmetric encryption is known as the single key encryption. RSA algorithm is a symmetric key encryption that uses public key and private key. Diffie-Hellman (DH) cryptography is where both parties exchange secrets keys to encrypt message. RSA and DH work differently but both are used for communicating between different parties.

Roy (2016) discussed that usage of internet is increasing all over the world. The author of this paper has highlighted the difference between the two encryption algorithms and further concluded that Asymmetric key cipher technique is way more secure compared to that of the symmetric key cipher technique. The author has also compared two prominent public key cryptography algorithms namely RSA algorithm as well as Diffie-Hellman algorithm and concluded that each such algorithm has its importance on particular context that leads to holding of advantage of each one over the other in case of a specific context.

Proposed Framework

The Diffie-Hellman Key Exchange algorithm has been demonstrated here. A tool CrypTool (Bernhard, 2007) has been used as simulator for the purpose. On the left side, the specific stages are given as follows:

a) Setting the public parameters
b) Choosing the secrets
c) Creating the shared keys
d) Exchanging the shared keys
e) Creating the common and secret key (session key)

The solution that propose here is designed to detect the Blackhole nodes in the default operations of either the intermediate nodes or that of the destination nodes. The approach follow, basically modifies the working of the source node and the change of the functioning of route reply using function broadcast the route reply (same like the route request function). In this proposed solution using a method called Prior_Receive Reply. In this method three things are added, a new table Reply-Table (Request Reply), a timer WT (Waiting Time) and a variable hackerNode (Malicious Node ID) to the data structures in the default AODV Protocol.

Metrics Involved

There are number of qualitative and quantitative metrics that can be used to compare reactive routing protocols. Most of the existing routing protocols ensure the qualitative metrics. The following metrics have been used for the analysis. These performance metrics determines the completeness and correctness of the routing protocol.

a) Packet Delivery Ratio: PDR is defined as a percentage of data packets delivered at receiver end compared to that of number of data packets sent for that node. It is used to measure the reliability, effectiveness and efficiency of routing protocols. Generally the reliability, effectiveness and efficiency of routing protocols can be improved by improving the PDR.

PDR = (DataR / DataS) * 100, Where

DataR = Data packets received by the CBR agent at destination node

DataS = Data packets Sent by the CBR agent at source node

b) Throughput: It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations.

c) Average end to end delay: The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination.

Average End-to-End Delay = (T_DataR – T_DataS), Where

T_DataR = Time data packets received at destination node

T_DataS = Time data packets sent from source node

d) Control packet overhead: The control packets are needed to establish route from the source to the destination. The control packets include RREQ, RREP and ERRP.

NRO = (CPSent + CPForw) / DataR, Where

CPSent = Control packets sent by all node

CPForw = Control packets forwarded by all nodes

DataR = Data packets received at the destination node

Conclusion

The effect on working of various mobility models has been investigated in different routing protocol that leads to the choice of mobility model, which is determined to give relatively better performance of different routing protocols. Authors studied various results to consider AODV as one of the best routing protocol for providing secure routing because there are almost best results in every scenario of the simulation as well as introduced a novel secure routing protocol.The proposed protocol is based upon hop count method from sender to target node. The scheme has been illustrated for AODV protocol and could easily be adopted for other on-demand routing protocols for providing stability, integrity and non-repudiation. The proposed algorithm has been evaluated with different network parameters under a simulated environment.

Future Work

The research work consistently requires a lot of hard work in order to maintain consistent energy of the nodes, send packets securely and safely across the network as well as to monitor the overhead packets. More comparisons are required with other schemes like DSR, TORA and other routing protocols. Power feature can also influence the study further as well as cryptography could be deeply analysed to prove a network error-free and secure.

References

1. Rahayu, T. M., Lee, S., Lee, H.,"A Secure Routing Protocol for Wireless Sensor Networks Considering Secure Data Aggregation", Sensors, ISSN: 1424-8220, Vol. 15, No. 7, pp. 15127-15158, 2015.

2. Akkaya, K., Younis, M.,"A Survey on Routing Protocols for Wireless Sensor Networks", Elsevier, Ad Hoc Networks, Vol. 3, Issue 3, pp. 325-349, May 2003.

3. Kurmi, J., Verma, R. S., Soni, S.,"An Approach for Data Aggregation Strategy in Wireless Sensor Network using MAC Authentication", Advances in Computational Sciences and Technology, ISSN: 0973-6107, Vol. 10, No. 5, pp. 1037-1047, 2017.

4. Merhi, Z., Haj-Ali, A., Abdul-Nabi, S., Bayoumi, M.,"Secure Localization for Wireless Sensor Networks Using Decentralized Dynamic Key Generation", 2012 8th

International Wireless Communications and Mobile Computing Conference (IWCMC), ISSN: 2376-6506, pp. 543-548, Limassol, Cyprus, 27-31 August 2012. DOI: 10.1109/IWCMC.2012.6314262.

5. Lal, N. A.,"A Review Of Encryption Algorithms-RSA And Diffie-Hellman", International Journal of Scientific & Technology Research, ISSN: 2277-8616, Vol. 6, Issue 07, July 2017.

6. Roy, A.,"Brief Comparison of RSA and Diffie-Hellman (Public Key) Algorithm", ACCENTS Transactions on Information Security, ISSN: 2455-7196, Vol. 1, Issue 1, pp. 28-31, 2016.

7. Bernhard Esslinger, "CrypTool, Version 1.4.10", Deutsche Bank AG, Frankfurt/Main, University of Siegen and Darmstadt, July 2007, www.cryptool.org.