Volume 3, Issue 4, April 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Synthesizing the Location by Providing Partial Privacy

Suganya Subathra. R
Dept. of CSE
Bharath University, India

Dhanarajan. S
Dept. of CSE
Bharath University, India

Harish. R
Dept.of CSE
Bharath University, India

Abstract- It is proposed for the evaluation of tradeoff between location privacy and energy efficiency in wireless sensor networks. Here, we consider that AODV (Ad-hoc On Distance Demand Vector) routing which is used to provide high energy efficiency and encryption algorithm that is used for providing partial privacy. We describe NS2, a simulation tool which executes a network daemon to generate high energy efficiency and low privacy by using symmetric algorithms key generate using static IP.

Keywords – Energy efficiency, privacy, Ad hoc Distance Demand Vector, Network Simulator, static IP.

I. INTRODUCTION

Wireless sensor networks are composed of independent sensor nodes deployed in an area working collectively in order to monitor different environmental and physical conditions such as motion, temperature, pressure, vibration sound or pollutants. The main reason in the advancement of wireless sensor network was military applications in battlefields in the beginning but now the application area is extended to other fields including industrial monitoring, controlling of traffic and health monitoring. Different constraints such as size and cost results in constraints in energy, bandwidth, memory and computational speed of sensor nodes. It has also the advantage over traditional networks in many ways. Moreover, it has increased fault tolerance because if a sensor node fails others can collect or process data. Because of its ad-hoc nature it becomes more attractive in certain applications. Nowadays, wireless sensor networks are broadly used in environmental control, surveillance tasks, monitoring, tracking and controlling, etc.

Routing protocols have been developed for ad hoc networks and have been categorized in two types of routing protocols namely reactive and proactive. In reactive routing protocols the routes are created only when source wants to send data to destination whereas proactive routing protocols are table driven Being a reactive routing protocol AODV uses traditional routing tables, one entry per destination and sequence numbers are used to determine whether routing information is secure communication channel, strong data encryption including secure communication channel, strong data up-to-date and to prevent routing loops. The maintenance of time-based states is an important feature of AODV which means that a routing entry which is not recently used is expired. The neighbors are notified in case of route breakage. The discovery of the route from source to destination is based on query and reply cycles and intermediate nodes store the route information in the form of route table entries along the route. Control messages used for the discovery and breakage of route are as follows:

- Route Request Message(RREQ)
- Route Reply Message(RREP)
- Route Error Message(RERR)
- HELLO Messages.

A.Route Request(RREQ)

A route request packet is flooded through the network when a route is not available for the destination from source. The parameters are source address, request ID, source sequence number, destination address, destination sequence number, hop count.

B.Route Reply(RREP)

On having a valid route to the destination or if the node is destination, a RREP message is sent to the source by the node. The following parameters are source address, destination address, destination sequence number, hop count, life time.

C. Route Error Message(RERR)

The neighborhood nodes are monitored. When a route that is active is lost, the neighborhood nodes are notified by route error messages(RERR) on both sides of sink.

D. Hello Messages

They are broadcasted in order to know neighborhood nodes. The neighborhood nodes are directly communicated. In AODV, messages are broadcasted in order to inform the neighbors about the activation of the link. These messages are not broadcast because of short time to live(TTL) with a value equal to one. In order to provide the location privacy, we go for the

encryption algorithm.Network Security & Cryptography is a concept to protect our network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. Cryptography terms like "codes" and "ciphers". Though many used both codes and ciphers interchangeably, but they are not the same. Users write a message with you own language, it is just a plaintext. If users want to make you plaintext message to make unintelligible to anyone other than us, then user use a cryptographic algorithm to encrypt the message. Actually, cryptographic algorithms encrypt a plaintext message into a cipher text message. Now, if user send that message to a person he can only read the message if he uses the same algorithm to decrypt it.

E. Symmetric Algorithms

A secret key algorithm is a cryptographic algorithm that uses the same key to encrypt and decrypt data. A form of encryption where the same key is used to encrypt and decrypt the text that is to be sent. This means that the sender and the receiver must have exchanged this key some time before the message has been sent and that this transfer must occur over a secure channel. The key used for symmetric key encryption is often known as a secret key. The algorithms used for encryption with this type of scheme can be either block cipher algorithms or cipher algorithms. The former encrypt a block of data at a time, while the latter encrypt data on a character-by-character basis. Symmetric key encryption algorithms are usually much more efficient than their main competitor, the algorithms used in public key encryption. Symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key).

F. Internet Service Providers

An ISP is a company that supplies Internet connectivity to home and business customers. ISPs support one or more forms of Internet access, ranging from traditional modem dial-up to DSL and cable modem broadband service to dedicated lines. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served. The larger ISPs have their own high-speed leased lines so that they are less dependent on the telecommunication providers and can provide better service to their . ISP is used as an abbreviation for *independent service provider* to distinguish a service provider that is an independent, separate company from a telephone company.

II. Related Work

In a formal model of the source-location privacy problem is provided, and two popular classes of routing protocols, namely, flooding protocols and single path protocol, are analyzed from the privacy and energy consumption. Based on such analysis a new technique called phantom routing is proposed that combines the advantages of both the above mentioned classes of routing protocols and provides suitable protection of the source location while not causing a noticeable increase in energy consumption. In the authors propose GROW (Greedy Random Walk): a two way random walk to reduce the change an eavesdropper can collect the source-location information. Note that both the above research contributions are simulation-based. In existing paper, we introduce an analytical framework for the evaluation of the tradeoff between location privacy and energy efficiency in wireless sensor network. To this end we extend the definition of privacy loss based on information theory concepts, proposed in for data mining system, to the case of location privacy in sensor network. More specifically, we focus on the relationship between random routing design choices and privacy loss as well as energy efficient. Accordingly, we will derive a Markov-based model of the random routing behavior that allows to calculate the privacy loss as well as the average energy consumption. Numerical results confirm that, as expected, energy efficiency and privacy are competing requirements. The framework can be used by protocol designers to set appropriate tradeoffs between the two above requirements. However, we use random routing it produces privacy loss.

In our proposed, Each route table entry contains the following information:

- Destination node
- Next hop
- Number of hops
- Destination sequence number
- Active neighbors for the route
- Expiration timer for the route table entry

The route discovery process is reinitiated to establish a new route to the destination node, if the source node moves in an active session. As the link is broken and node receives a notification, and Route Error (RERR) control packet is being sent to all the nodes that uses this broken link for further communication. And then, the source node restarts the discovery process.

Nodes within an ad hoc network generally rely on batteries (or exhaustive energy sources) for power. Since these energy sources have a limited lifetime, power availability is one of the most important constraints for the operation of the ad hoc network. There are different sources of power consumption in a mobile node.

Communication is one of the main sources of energy consumption. It should be noted that the energy consumed during sending a packet is the largest source of energy consumption of all modes.Since the rate of battery performance improvement is rather slow currently, and in the absence of breakthroughs in this field, other measures have to be taken to achieve the goal of getting more performance out of the currently available battery resources. Within this study, we focus our efforts on methods to reduce the power consumed in communications between ad hoc network nodes.

A.Key generate using static IP

Key generation is the process of generating keys for symmetric algorithms. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. Modern cryptographic systems include symmetric-key algorithms use a single shared key; keeping data secret requires keeping this key secret. A sender encrypts data with the public key; same key can decrypt this data. Computer cryptography uses integers for keys. In some cases keys are randomly generated using a *random number generator (RNG)* or *pseudorandom number generator (PRNG)*. A PRNG is a computer algorithm that produces data that appears random under analysis. In this stage Key generate using Static IP address is best way of solution.

Every cryptography has four basic goals-confidentiality, integrity, authentication and non-repudiation. Static IP using symmetric algorithm ensures that these four goals are met.

Privacy	Information must be kept from unauthorized parties
Integrity	Message must not be altered or tampered with
Authentications	Sender and recipient must prove their identities to each other
Non-repudiation	Proof is needed that the message was indeed received

Table-1 Cryptography Goals

B. Importance of Static IP address

- Web server's directly on user site that require external access
- E-mail server's directly on user site that require external access
- FTP server's directly on user site that require external
- DNS server's directly on user site that require external
- Application access requires external access
- Incoming Video or Audio services

Static IP address is a constant, The format of static IP address is easy identification receiver, sender's IP address (any doubt) gets and put their IP address ip2location .com and get senders identify geographical location, i.e. country, region, city, latitude, longitude, ZIP code, time zone, connection speed, ISP and domain name, IDD country code, area code, weather station code and name. This way of approach to easily server and client prove their identities. Non- repudiation gives assurances to the receiver of a message that it actually came from the sender and no one is faking the identity of the sender. This function of cryptography is provided with static IP address using symmetric algorithm only.

III. Experimental Result

In a particular network daemon, we can enhance the energy efficiency by using AODV routing protocol and providing the partial privacy by using key generate using static IP.

IV. Conclusion

Today the worldwide activities of various organizations, enterprises and institutions, general agencies and individuals are through network. The most important security to be given during communication is "unauthorized access". It is a very high level term refers to a number of difficult sorts of attacks. The goal of these attacks is to access important and valuable

resources from other machines. Hence network security pays an important role to product and prevents the unwanted access by other users, must be avoided in time.

V. Future Enhancement

In future work, we plan to undertake a greater exploration of various parameters and extensions to the described techniques. In particular, we intend to find how to provide enhanced levels of security whilst minimizing the energy consumption of sensor nodes in the presence of multiple attackers.

References

1. D. Dharmaraju. M. Rassi-Dehkordi, J. Jai/J. Baras, "Comparative Performance Evaluation of Routing Protocols for Mobile Ad Hoc Networks (MANETs)" University Of Mary land.
2. Z. Chang, G. Gaydadjiev and S. Vassilliadis, "Routing Protocols for Mobile Ad-hoc Networks: Current Development and Evaluation," Computer Engineering Laboratory, EEMCS, Delft University of Technology, Delft, Netherland.
3. L. Allazzawi, and A. Eikateeb, "Performance Evaluation Of WSN Routing Protocols Scalability," Vol: 2008, pp. 9.
4. G. Sklyarenko, "AODV Routing Protocol," Institut fur Informatik, Freie Universitat Berlin, Berlin, Germany
5. K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," Department of Computer Science and Electrica l Engineering, University of Maryland, Baltimore, Baltimore, U.S.A, 2003.
6. Y. Li, T. Newe, "Wireless Sensor Networks-Selection Of Routing Protocol For Applications," Department of Electric and Computer Engineering, University of Limmerick, Ireland.
7. Zurkinden, "Performance Evaluation of Routing Protocol: Real-Life Measurements," June, 2003.
8. V. Kunchakarra, "SIMULATION STUDY OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS," Department of Computer Science, Osmania University, Dec. 2005.
9. Dr. Prakash Ambegaonkar, "*Internet/Intranet Security.*" IEEE/ ACM Networking. December 2003
10. E.J.McGowAn,"*Intranet security 2003*",Software Development. April
11. Ferguson, Niels, and Schneier, Bruce – "*Practical Cryptography"*, Wiley, 2003, ISBN 0- 471- 22357-3.

