International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 1, Issue 1, September 2014

Energy and Security Enhancement in Wireless Sensor Networks using Sleep Awake Concept and AES

K.Praghash,
PG scholar, Department of Communication Systems, Francis Xavier Engineering College, Tirunelveli.
prakashcospra@gmail.com

Abstract - Unattended Wireless Sensor Networks (UWSNs) are defined by fixed or irregular intervals between sink visits and long periods of disconnected operations. Unattended Wireless Sensor Networks are more capable of providing computation, communication and power capabilities than peer to peer networks and ad hoc networks. UWSNs are mostly used for environment monitoring applications. An UWSN have thousands of sensors. Until their energy is depleted, these sensor nodes provide services throughout their whole lifetime. The existing WSN trust management schemes are not applicable to UWSNs when there is an absence of an online trusted third party implies that. To provide efficient and robust trust data storage and trust generation this method proposes a trust management scheme for UWSNs. To identify storage nodes and to significantly decrease storage cost, this method employs a geographic hash table for trust data storage. For mitigating trust fluctuations caused by environmental factors this method uses subjective logic based consensus techniques. It exploits a set of trust similarity functions to sustain trust pollution attacks and to detect trust outliers.

Keyword Terms: Unattended wireless sensor network (UWSN), distributed trust management, subjective logic

1.INTRODUCTION

The telecommunications network allows the computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections. Data is transferred in the form of packets. The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the Internet. Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as Ill as networking hardware. Two such devices are said

to be networked together when one device is able to exchange information with the other device,

whether or not they have a direct connection to each other. Computer networks differ in the physical media used to transmit their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent. In most cases, communications protocols are layered on (i.e. work using) other more specific or more general communications protocols, except for the physical layer that directly deals with the physical media. Computer networks support applications such as access to the World Wide Ib, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. A network is a group of two or more computer systems linked together. There are many types of computer networks. They are Local Area Networks, Wide Area Networks, Campus Area Networks, Metropolitan Area

Networks and Home Area Networks. Local-area networks (LANs) are the computers that are geographically close together (that is, in the same building). Wide Area Networks (WBNs) are the computers that are farther apart and are connected by telephone lines or radio waves. Campus-area networks (CANs) are the computers that are within a limited geographic area, such as a campus or military base. Metropolitan-area networks (MANs) are a data network designed for a town or city. Home-area networks (HANs) are a network that contained within a user's home that connects a person's digital devices. In cryptography, a trusted third party (TTP) is an entity which facilitates interactions between two

parties who both trust the third party; The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. In TTP models, the relying parties use this trust to secure their own interactions. TTPs are common in any number of commercial transactions and in cryptographic digital transactions as Ill as cryptographic protocols; for example, a certificate authority (CA) would issue a digital identity ceritificate to one of the two parties in the next example.

The CA then becomes the Trusted-Third-Party to that certificates issuance. Likewise transactions that need a third party recordation would also need a third-party repository service of some kind or another. Trust in Distributed and Peer-to-Peer Systems Reputation and trust systems in the context of distributed and peer-to-peer (P2P) networks are distributed.

2. EXSISTING CONCEPT: ADVANCED SCHEME

The Advanced Scheme (AS) utilizes a hash-table-like interface of GHT where nodes can put and get data based on their data type, i.e., Put(Data Type, Data Value) and Get(Data Type). Since a sensor ID is unique in the network, trust producers are able to put trust opinions to trust managers based on the ID, i.e., Put (s_j, $T_i^{j,t}$). Trust consumers are able to get trustworthiness from trust managers using the same sensor ID, i.e., Get (s_j). In other words, trust opinions are pushed by, and stored at the same trust manager node. Meanwhile it enables trust consumers to pull trustworthiness from the trust manager nodes consistently. Neither trust producers nor trust consumers need to store the IDs of trust manager nodes, reducing storage cost significantly. Furthermore, the scheme should not be sensitive to node failures. That is, the scheme should be resilient to ADV_Del. Using the Get(s_j, r) function, trust consumers are able to get s_j's trustworthiness □^{j} from the r-th trust manager node of s_j. That is, each node has α trust manager nodes to store its trust opinions from its neighbors for data redundancy. Trust opinions regarding a sensor s_j are hashed by the sensor ID s_j to a geographical location. The node closest to the hashed geographical location is referred to as the trust manager node where data is sent to and retrieved from.

The closest node to the location L_j^r, namely trust manager can receive the trust opinions and trust query requests. The AS includes the following phases:

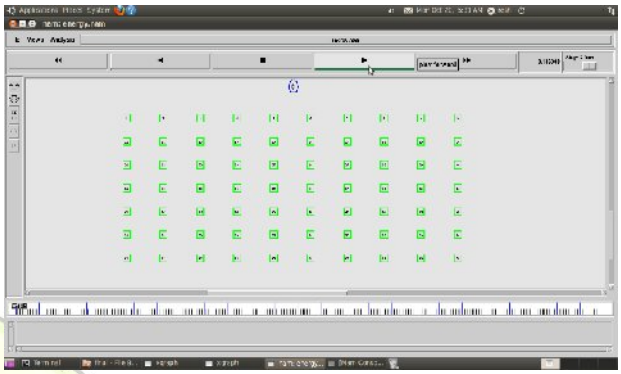

Fig .1 Network Based on Advanced Scheme

3. SLEEP-AWAKE CONCEPT

The high level design goal of snooze & stir is to loosen up the hypothesis that every node knows the location of its first and second-hop neighbours, and to streamline the rouse-up hardware and stir indicator. Again meanwhile snooze & up practices the resulting steps to stir the sentries along the track from Source to Destination:

1. The Source node disseminates a stir indicator to all its first-hop neighbours. The stir indicator comprises the mutual uniqueness of the existing transmitter (T1), the later hop (h1), and the prior hop (void on behalf of T1).
2. Every neighbours of T1, after stir, concludes whether to remain up or go back to snooze based on the responsibility that it may take part in the enduring communication. If that neighbour is the later hop (h1), it remains up to advance the data and to observe the later hop from it for the later hop h1 above the connection h1n2, it remains up to observe the activities of h1. If the node is a sentry of a advancing node over the prior hop, it remains up to spot assembly by the advancing node. A node autonomously can make this fortitude based on first and second hop neighbour statistics. If no one of these instances retain, the node goes back to snooze instantly.
3. Node T1 delivers the data packet to h1 resulting the timing reservation given
4. Nodes h1 after being stir maintain to remain up for Tw. Afterward, it drives posterior to snooze.

5. H1 does the unchanged steps that T1 did to stir the later hop (h2) and h1's sentries
6. If h1 crashes to transmit the stir indicator, the sentry of h1 with the truncated PERMIT transmits a dual hop dissemination of the stir indicator concluded. If that sentry crashes, the sentry with the later smallest PERMIT transmits the indicator, and so on. This layout certifies that if there is a sequence of scheming malicious nodes then all the nodes will be distrusted.
7. The practice continues at all step till the endpoint. This design concludes in a decrease in the energy utilisation.

4.CONCLUSION

In the exsisting scheme, an efficient and robust trust management schemes for UWSNs based on Subjective Logic is introduced. This advanced trust storage scheme (AS) facilitates distributed trust data storage to ensure high reliability of trust data. It takes the advantage of both GHT and GPSR routing to find storage nodes and to route trust data.

I have also proposed several methods to mitigate trust pollution attacks based on various trust similarity measures.

I demonstrated that our trust management schemes are resilient to major attack categories including ADV_Del, ADV_Noise, ADV_Homo, and ADV_Hbd. Moreover, the simulation results demonstrated that AS has much loIr storage costs compared with the less sophisticated approaches. Combining AS with similarity threshold measures, these schemes are able to significantly reduce trust storage costs and perform efficient node invalidation and mitigation of ADV's pollution attacks.

5. REFERENCES

[1]. A. Ma, C. Soriente, and G. Tsudik, "New adversary and new threats: Security in unattended sensor networks," IEEE Netw., vol. 23, no. 2, pp. 43–48, Mar. 2009.
[2]. C.. Ren, V. Oleshchuk, F. Y. Li, and S. Sulistyo, "SCARKER: A sensor capture resistance and key refreshing scheme for mobile WSNs," in Proc. IEEE LCN, Bonn, Germany, 2011.
[3]. E. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Catch me (if you can): Data survival in unattended sensor networks," in Proc. IEEE PERCOM, Hong Kong, 2008.
[4]. E. Di Pietro, G. Oligeri, C. Soriente, and G. Tsudik, "United I stand: Intrusion-resilience in mobile unattended WSNs," IEEE Trans. Mobile Comput., vol. 12, no. 7, pp. 1456–1468, Jul. 2013.