International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 5; Issue: 6; June-2016

An Efficient and Secure Data Dissemination Protocol for Wireless Sensor Network

Aneesa Fatima[1], Gururaj Nase[2]
[1]*PG Student, Department of Computer Science and Engineering,*
[2]*Assistant Professor, Department of Computer Science and Engineering,*
Lingaraj Appa Engineering College, Bidar, Karnataka State, India.

***Abstract*— In the large number of outgrowing commercial environment each and everything depends on the other sources to transmit the data securely and maintain the data as well in the regular medium. Portable nodes in military environments, for example, a front line or an antagonistic area are prone to experience the undergo of irregular system network and frequent partitions. Disruption-tolerant network (DTN) innovations are getting to be fruitful results that permit remote device conveyed by officers to speak with one another and access the confidential data or secret data or summon dependably by abusing outside capacity nodes or storage nodes. Thus a new methodology is introduced to provide successful communication between each other as well as access the confidential information provided by some major authorities like commander or other superiors. The methodology is called Disruption-Tolerant Network (DTN). This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases. The most promising cryptographic solution is introduced to control the access issues called Cipher text Policy Attribute Based Encryption (CP-ABE). Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a guaranteeing cryptographic answer for the right to gain entrance control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to safely and proficiently deal with the classified information dispersed in the Interruption or disruption tolerant network.**

***Keywords*— Distributed data discovery and dissemination, security, wireless sensor networks, efficiency.**

I. INTRODUCTION

Wireless sensor network (WSN) is deployed there is usually a need to update buggy old small programs or parameters stored in the sensor nodes. This can be achieved by the data discovery and dissemination protocol, which facilities a source to inject small programs, commands, queries and configuration parameters to sensor nodes. Note that it is different from the code dissemination protocols which distribute large binaries to reprogram the whole network of sensors. For example, efficiently disseminating a binary file of tens of kilobytes requires a code dissemination protocol. While disseminating several two-byte configuration parameter requires data discovery and dissemination protocol. Considering the sensor nodes could be distributed in a harsh environment, remotely disseminating such small data to the sensor nodes through the wireless channel is a more preferred and practical approach than manual intervention. Motivate by the above observation, this paper as the following main contribution 1 the need of distributed data discovery and dissemination protocol is not completely new, but previous work did not address this need we study the functional requirement of such protocol, and said there design objective. Also we identify the security vulnerabilities in existing data discovery and dissemination protocol.

WIREIESS SENSOR NETWORK

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

ROUTING IN WIRELESS SENSOR NETWORK

Due to recent technological advances, the manufacturing of small and low cost sensors became technically and economically feasible. The sensing electronics measure ambient conditions related to the environment surrounding the sensor and transform them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of+ the sensor. A large number of these disposable sensors can be networked in many applications that require unattended operations. A Wireless Sensor Network (WSN) contains hundreds or thousands of these sensor nodes. These sensors have the ability to communicate either among each other or directly to an external base-station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy.

In the past few years, an intensive research that addresses the potential of collaboration among sensors in data gathering and processing and in the coordination and management of the sensing activity were conducted. However, sensor nodes are constrained in energy supply and bandwidth. Thus, innovative techniques that eliminate energy inefficiencies that would shorten the lifetime of the network are highly required. Such

constraints combined with a typical deployment of large number of sensor nodes pose many challenges to the design and management of WSNs and necessitated energy-awareness at all layers of the networking protocol stack. For example, at the network layer, it is highly desirable to find methods for energy-efficient route discovery and relaying of data from the sensor nodes to the BS so that the lifetime of the network is maximized.

II. Related Work

As a special sensor network, a wireless body area network (WBAN) provides an economical solution to real-time monitoring and reporting of patients physiological data wireless sensor networks are widely data applicable in monitoring and control of environment parameters. It is sometimes necessary to disseminate data through wireless links after they are deployed in order to adjust configuration parameters of sensors or distribute management commands and queries to sensors. Several approaches have been proposed recently for data discovery and dissemination in WSNs. A data discovery and dissemination protocol, for wireless sensor networks (WSNs) is answerable for updating configuration parameters of, and distributing management instructions to, the sensor nodes. All existing data discovery and dissemination protocols undergo from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data item.

Wireless sensor networks (WSN) are attractive for information discovery in large-scale data rich environments and can add value to mission-critical applications such as battle-field surveillance, environmental monitoring and emergency response. However, in order to fully exploit these networks for such applications. Data dissemination and discovery is critical for ad-hoc wireless sensor networks. Most existing research depends on location information that is not always obtained easily, efficiently and accurately. We propose the concept of Contour-cast, a location-free data dissemination and discovery approach for largescale wireless sensor networks. Multidimensional WSNs are deployed in complex environments to sense and collect data relating to multiple attributes (multidimensional data). Such networks present unique challenges to data dissemination, data storage and in-network query processing (information discovery). we present simulation results showing the optimal routing structure depends on the frequency of events and query occurrence in the network. It also balances push and pulls operations in large scale networks enabling significant QoS improvements and energy savings. Multicast communication is becoming the basis for a growing number of applications. Therefore, securing multicast communication is a strategic requirement for effective deployment of large scale business multi-party applications. One of the main issues in securing multicast communication is the source authentication service. Sensor networks deployed in hostile areas are subject to node replication attacks, in which an adversary compromises a few sensors, extracts the security keys, and clones them in a large number of replicas, which are introduced into the network to perform insider attacks.

III.PROPOSED SYSTEM

DiDrip consists of four phases, system initialization, user joining, and packet pre-processing and packet verification. For our basic protocol, in system initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. In user joining phase, a user gets the dissemination privilege through registering to the network owner. In packet pre-processing phase, if a user enters to the network and wants to dissemination some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet. Based on the design objectives, they propose DiDrip. It is the first distributed data discovery and dissemination protocol, which allows network owners and authorized users to disseminate data items into WSNs without relying on the base station. Moreover, our extensive analysis demonstrates that DiDrip satisfies the security requirements of the protocols of its kind. In particular, they apply the provable security technique to formally prove the authenticity and integrity of the disseminated data items in DiDrip.

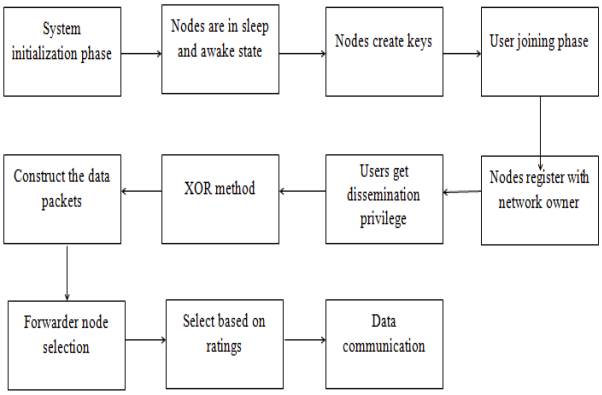

Fig.1 Block diagram of Proposed System

In this paper, in order to enhance the security and mutual authentication to each and every node, a trust based model is followed. According to this method, the rating of each node is maintained at each node level. The ratings of a node will be done through the ratio of packet forwarded by packets received. The node selection is based on the ratings. The nodes which are having high-rating are considered as trusted one and data packets are routed through them.

IV. IMPLEMENTATION

DiDrip Protocol mainly includes five phases to disseminate the data between the nodes among the wireless sensor network. Figure 1 shows the system architecture for DiDrip Secure protocol, which shows the data discovery and dissemination of data from source to destination through the authorized users only, where it contains the following mechanisms.

- Network Owners
- Authorized users
- Sensor nodes

Advantages

- Proposed approach is suitable for multi-owner-multi-user WSNs.
- Identified the security vulnerabilities in data discovery and dissemination when used in WSNs.

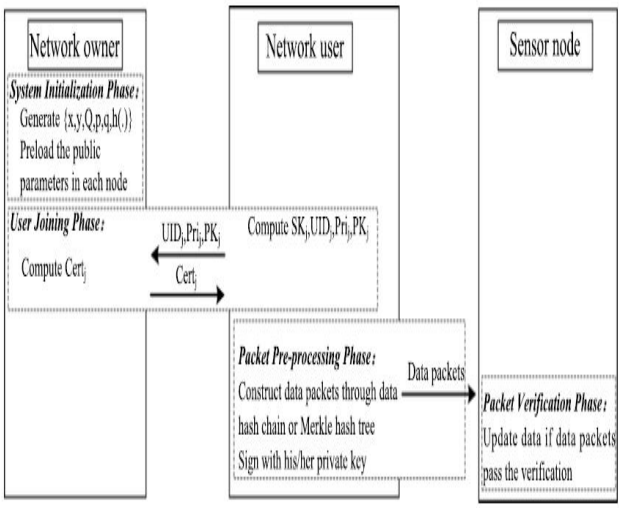

Fig. 3 Information processing flow in DiDrip

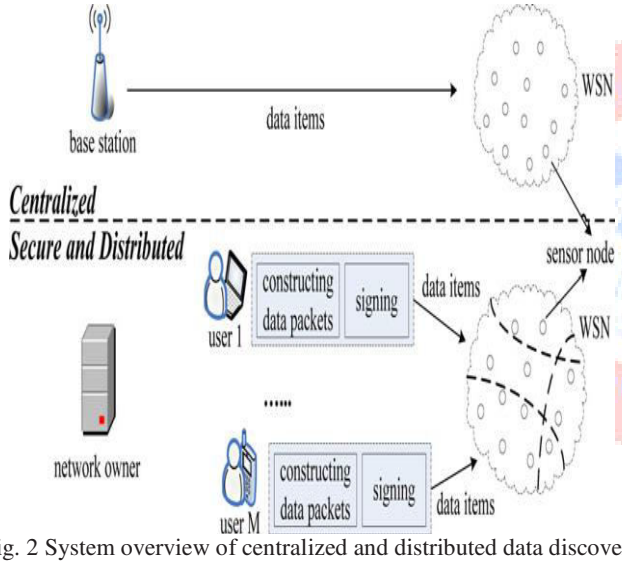

Fig. 2 System overview of centralized and distributed data discovery and dissemination approaches

Notation	Description
UID_j	Identity of user U_j
PK_j	Public key of user U_j
SK_j	Private key of U_j
Pri_j	Dissemination privilege for user U_j
$Cert_j$	Certificate of user U_j
$SIG_k(M)$	Signature on message M with key k
h(M)	Hash value of message M
$\|$ or ,	Concatenation of two bit streams

TABLE 1: Notations

The protocol consists of four phases namely, system initialization phase, user joining phase, packet pre-processing phase and packet verification phase each of which are described in detail in the following sub-sections. The Table 1 shows the notations that are used in the description. The flow of information processing at network owner, network user and sensor nodes is shown in Fig. 2.

A. ***System Initialization Phase***

160 bit Elliptic curve cryptography is set up in this phase. The network owner performs the following steps.

- Choose two big prime numbers p and q each of 160 bits long.
- Select an elliptic curve E over GF(p)
- Select private key x ϵ GF(q).
- Compute the public key y = xQ where Q is the base point of E and is of 320 bits long. y is 160 bits long.
- Load the public parameters {y, Q, p, q} in each node.

B. User Joining Phase

When any user, say Uj wants to join the network and obtain the dissemination privileges, the user joining phase is invoked.

The user requests for the certificate from the network owner. The steps are as follows.

- Consider a network user U_j with the identity UID_j which is of two bytes.
- User chooses a private key $SK_j \in GF(q)$
- User computes the public key $PK_j = SK_j.Q$
- User sends a 3-tuple $< UID_j, Pri_j, PK_j >$ to the network owner.
- The network owner generates the certificate and sends back to the user U_j.

$Cert_j = \{ UID_j, PK_j Pri_j, SIG_x\{h(UID_j \| PK \| Pri_j)\}\}$

Since user ID is of two bytes, 65,536 users can be supported. The length of privileges field is of 6 bytes andhence the certificate generated is 88 bytes long.

C. Packet Pre-processing Phase

When a user enters the network and has some information to disseminate over the network, first it has to construct the packet. This is done in packet pre-processing phase. The following steps are performed.

- The user constructs the packet by using Merkle hash tree method.
- Here a tree is constructed taking n data items.
- The data items act as the leaves of the tree.
- At the upper level, internal nodes are constructed by concatenating two child nodes.
- Continue constructing the nodes until the root node is formed. It is labelled as H_{root}.
- Thus obtained tree is the Merkle hash tree with depth $D = \log_n(n)$.
- The user, before dissemination of actual data items,
- Signs the root node $H_{root}$with SK_j.
- Sends an advertisement packet P0
  $P0 = \{Cert_j \| H_{root} \| SK_j(H_{root})\}$
- After sending P0, the user disseminates further packets along with the appropriate internal nodes. In Merkle hash tree method, each packet contains the D hash values.

D. Packet Verification Phase

When any sensor node receives the disseminated data, it has to first verify whether it is from authorized user, whether that sensor node ID is included in the node identity set of Pri_j and whether the packet maintains data integrity. The following steps are performed.

- If the packet received is advertisement packet
  $P0 = \{Cert_j \| H_{root} \| SK_j(H_{root})\}$, check for the privileges.
- If the result is positive, then check for the authenticity if certificate by using the public key, y of the network owner.
- If certificate is valid, check for the validity of signature.
- If the result is positive then store $<UID_j, root>$, otherwise discard the packet.
- If the packet received is a data packet other than P0, the sensor node checks for the authenticity and integrity.
- For positive result, it checks for the freshness of the data. If the packet received is a newer version, then it updates its data.

V. RESULTS

After implementing the proposed system on NS2 platform, the results obtained are as follows:

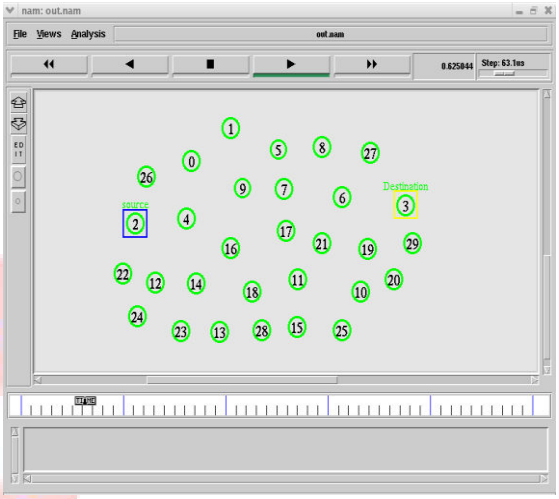

Fig.4 Network Creation

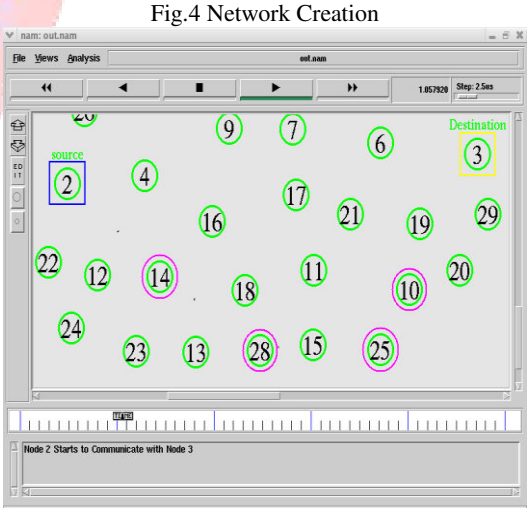

Fig. 5 Communication Stage

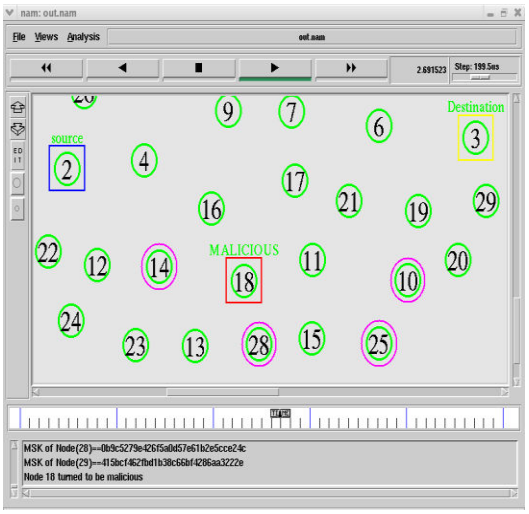

Fig. 6 Malicious Node attack

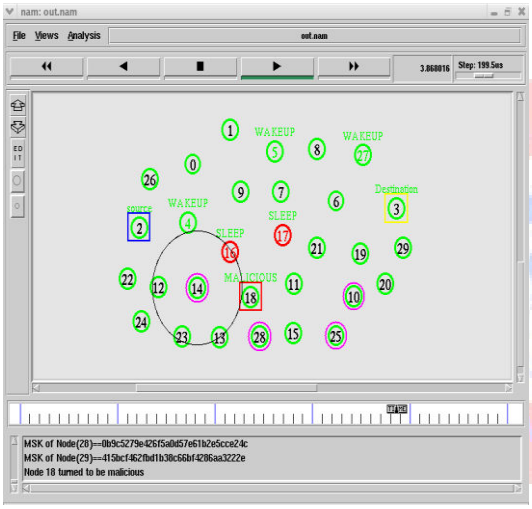

Fig. 7 Nodes with Sleep and Awake states

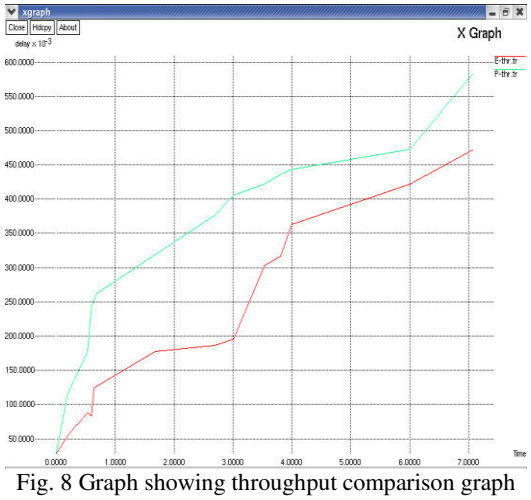

Fig. 8 Graph showing throughput comparison graph

Fig. 9 Graph showing delay comparison graph

VI. CONCLUSIONS

In this paper, we have identified the security vulnerabilities in data discovery and dissemination when used in WSNs, which have not been addressed in previous research. Also, none of those approaches support distributed operation. Therefore, in this paper, a secure and distributed data discovery and dissemination protocol named DiDrip has been proposed. Besides analyzing the security of DiDrip, this paper has also reported the evaluation results of DiDrip in an experimental network of resource-limited sensor nodes, which shows that DiDrip is feasible in practice. We have also given a formal proof of the authenticity and integrity of the disseminated data items in DiDrip. Also, due to the open nature of wireless channels, messages can be easily intercepted. Thus, in the future work, we will consider how to ensure data confidentiality in the design of secure and distributed data discovery and dissemination protocols.

REFERENCES

[1] J. W. Hui and D. Culler, "The dynamic behavior of a data dissemination protocol for network programming at scale," in Proc. ACM SenSys, pp. 81-94, 2004.
[2] D. He, C. Chen, S. Chan and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946-1956, May 2012.
[3] T. Dang, N. Bulusu, W. Feng and S. Park, "DHV: A code consistency maintenance protocol for multi-hop wireless sensor networks," in Proc. EWSN, pp. 327-342, 2009.
[4] G. Tolle and D. Culler, "Design of an application-cooperative management system for wireless sensor networks," in Proc. EWSN, pp. 121- 132, 2005.
[5] K. Lin and P. Levis, "Data Discovery and Dissemination with DIP," in Proc. ACM/IEEE IPSN, pp. 433-444, 2008.
[6] M. Ceriotti et al., "Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment," in Proc. IEEE IPSN, pp. 277- 288, 2009.
[7] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks,"

IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638-4646, Sept. 2013.
[8] S. Rahman, N. Nasser, T. Taleb, "Secure timing synchronization for heterogeneous sensor network using pairing over elliptic curve," Wireless Communications and Mobile Computing, vol. 10, no. 5, pp. 662-671, May 2010.
[9] M. Rahman, N. Nasser, and T. Taleb, "Pairing-based secure timing synchronization for heterogeneous sensor networks," in Proc. IEEE GLOBECOM, pp. 1-5, 2008.
[10] Geoss. http://www.epa.gov/geoss/.
[11] NOPP, http://www.nopp.org/.
[12] ORION, http://www.joiscience.org/ocean observing/advisors.
[13] P. Levis, N. Patel, D. Culler and S. Shenker, "Trickle: A self-regulating algorithm for code maintenance and propagation in wireless sensor networks," in Proc. NSDI, pp. 15-28, 2004.
[14] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Effcient and secure source authentication for multicast," in Proc. NDSS, pp. 35-46, 2001.
[15] Y. Chen, I. Lin, C. Lei and Y. Liao, "Broadcast authentication in sensor networks using compressed bloom filters," in Proc. DCOSS, pp. 99-111, 2008