RESEARCH ARTICLE OPEN ACCESS

Data Security and Data Dissemination of Distributed Data in Wireless Sensor Networks

M. Kowsigan[1], M.Rubasri[2], R.Sujithra[2], H.Sumaiya Banu[2]

[1]*Assistant professor, Department of Information Technology, Sri Krishna College of Technology, Coimbatore, India*

[2]*Department of Information Technology, Sri Krishna College of Technology, Coimbatore, India*

ABSTRACT

A data dissemination protocol for wireless sensor networks has been engaged for modifying configuration fields and circulating management controls to the mote. Earlier, a data dissemination protocol faces the henceforth two consequences. First, they are works on sink based model; only the sink can circulate data item to other motes. Such model is not suitable for large user wireless sensor networks. Second, those protocols are not provide with any security and hence intruders will make problems to misuse the network. We provided the seDrip protocol. It allows the network mentors to authorize multiple network uses with various permissions to simultaneously and directly distributed data items to the mote. seDrip is implemented in an laboratory of network restricted resources mote to depict its large capability in practice.

Index Terms: data security, seDrip, capability.

I. INTRODUCTION

Wireless sensor network is necessary to change small codes or fields stored in the wireless mote. These could be gained by the data dissemination protocol, which facilities a sender to insert small codes, commands and configuration fields to mote. It varies from the code dissemination protocol which circulates large binals to the entire network of sensor nodes. Example, effectively disseminating a binal files of kilobytes requires a code disseminating protocol. When disseminating various two-byte configuration field needs data dissemination protocol.

Considering mote would be circulated in an environment, remotely transporting such small amount of data to the mote through the wireless communication is mostly accepted and visual approach than manual implementation. functional requirement of such protocol, and said there design objective. Also we found the authenticationissues in existing data dissemination protocol.

II. A BRIEF LITERATURE REVIEW

There has been a large body of research on WSNs in the literature. In the following, we outline the research issues that have been actively pursued by the researchers.

Pairing-based secure timing synchronization for heterogeneous sensor networks: These papers consider HSNs as a model for our proposed novel time synchronization protocol based on pairing and IBC. This is the first approach for synchronization protocol using pairing based cryptography in HSNs. The proposed scheme reduces the key space of mote as well as it prevents from all security attacks.

TinyECC: A configurable library for ECC in wireless sensor networks. This paper presents the design and implementation of TinyECC, a configurable library for ECC operations in WSNs. The objective of TinyECC is to provide a ready-to-use, publicly available software packages for ECC based operations that can be flexibly configured and integrated into sensor network applications. The evaluation results show the impact of individual optimizations on the execution time and resource consumption and give the most computationally efficient and the most storage efficient configuration of TinyECC.

Monitoring heritage buildings with WSNs: The Torre Aquila deployment:It shows that our system is an effective tool for assessing the tower's stability, as it delivers data reliably (with loss ratios less than 0.01%) and has an estimated lifetime.

DiCode: DoS resistant and distributed code dissemination in WSNs.This paper develops a secure and distributed code dissemination protocol named DiCode. A salient feature of DiCode is its ability to resist denial of service attack which have severe consequence on network availability. Performance analysis wireless OCDMA systems had been done in [12]. Further, the security properties of our protocol are demonstrated by theoretical analysis.

Secure data discovery based on hash tree for wireless sensor networks:This paper identifies the security problems in data discovery and dissemination when used in wireless sensor networks. An efficient job scheduling was implemented and it performs useful task regarding to the wireless sensor networks [10][11]. Such problems allow an adversary to update a network with undesirable values and erase critical variables or launch denial of service (DoS) attacks. To address these attacks this paper presents the design, implementation and evaluation of secure, lightweight and DoS resistant data dissemination protocol named diDrip for WSNs.

III. PROPOSED SYSTEM

To protect wireless sensor networks from security issue, we introduce an improved filtering technique. Those techniques make them not only collision robust but also more accurate and faster converging. In our proposed work we increase data level security by introducing asymmetric key encryption. Using RSA algorithm we provide security in data. The suggested protocol is efficient in a multi-scale WSN.Distributed seDrip, which permits the network mentors and authenticated users to distribute data items into WSNs without depending on the sink. Our dedicated analysis states that SeDrip will satisfy the authentication needs of the protocols of this kind. In particular, we applied some of the algorithms to provide the authenticity and integrity of the disseminated data items in SeDrip.

IV. WIRELESS SENSOR NETWORK

A wireless sensor network contains a circulated independent mote to analyze physical conditions such as environment, noise, pressure to co-operatively send their informationpasses by the network to a particular location. The present networks are bi-directional and also controls the sensor activity. The development of WSN were developed in inspirationwith applications used in military increased fields [7]. Now-a-days WSNs are employed in several industries and commercial applications.

A.Routing In Wireless Sensor Network

In connect with many recent technological advancements, the evolution of a very small and low cost sensors became possible. The sensing electronics measures the medium conditions in relation with the environment surrounding the mote and converts them into an electric signal. Processing such signals shows few properties about information located and things happening around of the mote. Genetic algorithm was used as one of the tool for routing the jobs in cloud [14].These motes have the capability to transmit among each other or to an external sink. A great number of sensor motes allows for sensing over a large area with a greater exactness.

Few years back, an exhaustive research that labels the potentiality in association with sensors in data gathering, data handling activities were conducted. Motes are confined in the energy distribution and in the bandwidth. Thus, innovative techniques removes energy incompetent that could shorten the life of the network are largely required. Such confined combining with an assessing of huge number of mote pose various issues to the develop and manage the wireless sensor networks at all layers of the networking protocol stacks.

Routing in wireless sensor networks is demanding the inherent characteristics that distinguish the networks from external wireless networks such as mobile ad hoc networks or cellular networks. Due to the many of the motes, building a global level addressing scheme is not possible for the evolvation of nodes in sensor network as the overhead of ID maintenance is high.

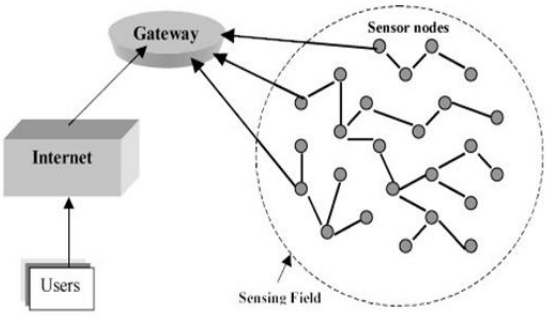


Fig 1: Wireless Sensor Network

B.Multi-Path Routing Protocols

We examine the routing protocols which uses multiple paths rather than a unidirectional way in account to enhance the network's performance. The fault tolerance of a protocol is evaluated by the probability of a different path existing between a sender and a receipt when a primary path fails. These alternative paths are kept active by passing repeated information. Hence, the network authenticity can be enhanced at the cost of enlarging overhead of retaining the alternative paths. Handling spread is a good for powerful multi-path routing. Ground of the handling spread function, a multi-path routing protocol that finds a various slightly separated paths. It found that the application of multi-path routing protocol provides viable alternate for energy efficient recovery from failures in a wireless sensor networks. The motivation of using these to retain the expense of supervising each and every other paths low.

V.INTRODUCTION TO NETWORK

NS2 is a simulation tool aiming at both the local and the satellite networking research. Network Simulator is a very promising tool which is being used by scholars and universities. We provided information in steps to setup NS2 on UNIX. Then we have scrutinized how to implement NS2 to simulate limited and wide area networks. We discussed both the methods. Multimodal Personal Authentication with Fingerprint, Speech and Teeth Traits using SVM Classifier [13]. Finally, the methods to animate uses NAM and to analyze it uses X graph / GNU picture the simulation results are presented.

NS, a separate event simulator at the network research is used in companies by scholars and universities. Network Simulator provides background needs for simulation of transmission control protocol, multi-cast protocols, and routing over limited and wide area networks. It deploys network protocols such as file transfer protocol and Telecommunication network, routing algorithms such as DV and SPF.

A simple way NS2 could be applied to study the characteristic of a well-known protocol. A script language OTcl is employed to glue the network components such as nodes, links, agents, applications, etc which are provided by NS2, configure the parameters such as band-width, delay, routing protocol, etc and launch activities (data transfer, topology change, etc). NS2 will read the configurations; simulate the network event and record event and statistics in to the trace files. After the simulation, Nam method can demonstrate the events in a visualized way.

VI. NETWORK FORMATION AND COMMUNICATION IN WSN

In this module designing of complete WSN will be done and the number of Mote, cluster node and gateway node and then interrelate them to form the network. Once, designing of Wireless Sensor Networks is completed, and then the next step is to have the communication between each node [9]. The communication in the sense there will be transmission of the data amongst different motes in the network. The proposed module will emphasize on distribution of data security and dissemination protocols and the functional requirements of such protocols, it sets their design objectives [15]. It identifies the security problems in predefined data dissemination protocols. The communication in the sense there will be transmission of the data amongst different motes in the network. The module is a RSA asymmetric key algorithm.RSA is the leading in the known general service asymmetric key algorithm. This had been created by Rivest, Shamir & Adleman of MIT. It is depend on exponentiation in a known range over integers modulo a prime, using huge integers leads up to 1024 bits. Its security is due to the amount of factorizing huge numbers. In RSA algorithm, to encode a plain text P the sender should obtains asymmetric key of receiver PU={s, r} and by using that computes cipher text $T = P^s \bmod r$, where $0 \leq P < r$ to encode the plain text. To find decoding key k applied the following equation $s.k=1 \bmod ø(r)$ and $0 \leq k \leq r$.After those steps publish their asymmetric encoding key, PU={s, r} and keep secret private decoding key, PR= {k, r} in source and destination side.For this algorithm to be satisfactory for asymmetric key encoding, it must be possible to find values of k, s, r such that $P^s k \bmod r = P$ for all $P < r$. We need to find a relation of the form Pkd *mod r = P*. The preceding relation stands if *s and k* are inverse multiplication mod *ø (r),* where *ø (r)* is a totient function. This is the straight reaction of Euler's function, so that taking a number to power s then k or vica versa produces the original number.

VII. SECURITY ANALYSIS

In the following, we will analyze the security of seDrip to verify that the security requirements. To pass the verification of mote, each user has to submit the secrete key and the dissemination permissions to the network provider for registration. Authorized users are capable to process data dissemination in a circulated manner with a Support of various user permissions [6]. Activities of users in a network can be restricted by setting user permission Prij, which is included in the user certificate. Since each user certificate is created based on Prij, it will not pass the verification at mote if Prij is modified. Thus, only the network mentors can modify Prij and then updates the certificate accordingly to provide authenticity and integrity of the data items. With the RSA Algorithm, an authorized user signs the data into SHA(Secure Hash Algorithm) with their secrete key [3]. Using the network provider's asymmetric key, each mote can validate the user certificate and obtains the user's asymmetric key. Then, using the user's asymmetric key, each mote can validate the data packet received and other data packets regarding Secure Hash Algorithm. With the assumption that the network provider cannot be compromised, it is guaranteed that all forged or modified data items can be very simply founded by the authentication process. User accountability, Users identities and the data dissemination activities are exposed to wireless sensor nodes. Thus, the mote can report such records to the network provider periodically. Since each user certificate is created regarding to the user id, except the network provider, no one can modify the user identity specified in the user certificate which will pass the authentication. Therefore, the users should not repudiate their activities, Node compromise and user collision tolerance. As described above, for basic the protocol, only the asymmetric arguments are preloaded in each and every node. Also for the enhanced protocol, the dissemination-privilege set of a network user is loaded into the mote. Therefore, not important how many number of mote are being used, the adversary just obtains the asymmetric arguments and the dissemination- privileged set of a user. The intruder does not make any issue by compromising mote. A few users conspire; a benign node will not permit any dissemination privilege that is beyond those of conspiring users. This property Resistance to DoS(Denial-of-Service) attacks. There are Denial-of-Service attacks takes upon basic Data dissemination protocol by exploiting the authentication delays, signature verifications and the Trickle algorithm [1].

First, by applying Secure Hash Algorithm, each mote can efficiently validate a data packet by a few hash operations. Second, using the 160 bit message digest we can securely transfer data in a efficient manner[8]. Therefore, all the above DoS attacks are defended. SeDrip can successfully defeat all three types of Denial of services attacks with a presents of a compromised network users and mote. Without knowing the secret key and the asymmetric keys of the network users, even an inside attacker cannot forge any data packets with ensure of freshness[4]. Thus we will consider how to implement data confidentiality in the model of secure seDrip and RSA algorithm. This system will maintain the data integrity also to ensure the performance of the system[5]. Here we can conclude that the proposed system will provide the high security. Then by applying energy efficient SHA algorithm we will encode and decode the plain text for the security purpose. We applied SHA and RSA algorithm to represent a security process for wireless sensor networks which is simple to implement as well as impossible to break. In this research we are simply going to provide secure communication, but we will also reduce the energy inefficiencies by providing gateway nodes, which will make the system much more protected and reliable. This will provide us a high security to the wireless sensor network by detecting and sending secrete data to the recipient only from a source by applying authentication on data[2].

VIII. SYSTEM REQUIREMENTS

To be utilized productively, all PC programming needs certain apparatus segments or any programming assets to be available on a PC. These are known as PC framework essentials and are simultaneously applied as a procedure instead of a flat out standard. Many programming uses least and prescribed arrangements for framework precondition,. With enlarging interest for higher handling force and belonging in more up to date variants of programming, framework precondition tend to increment after some time. Industry examiners recommend that this pattern have affected largely in propulsive moves up to existing PC frameworks than inventive progressions.

A.Software Requirements

- Operating system : Linux (Ubuntu)
- Software : Network Simulator 2.35
- Coding : TCL, AWK, C++

B.Hardware Requirements

- Main processor : Dual Core
- Hard disk capacity : 60GB
- RAM memory : 4 GB

IX. IMPLIMENTATION DETAILS

seDrip mainly includes five steps to disseminate the data between the motes among the wireless sensor network. Figure2 depicts the structure of secure SeDrip, which shows the dissemination of data from source to destination through the authorized users only. where it contains the following mechanisms:

- Network mentors
- Authorized users
- Mote

Advantages

- Applicable for multi-owner with multi-user WSNs.
- Identified the security issues in data dissemination protocol when used in WSNs.

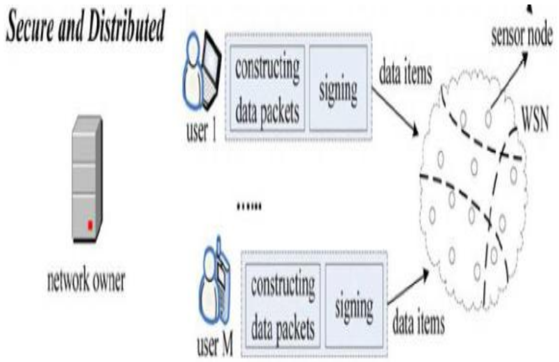
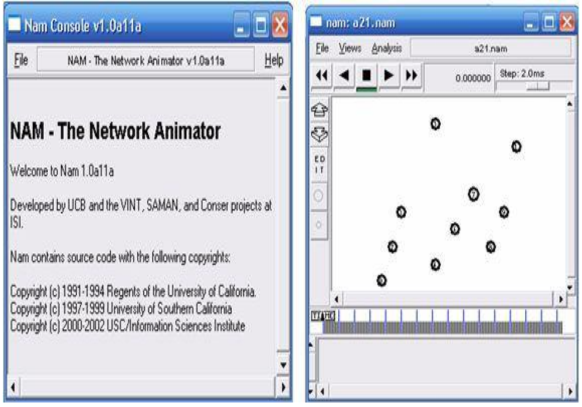


Fig 2: Structure of secure seDrip

SeDrip consists of four phases, data model, user entering, and packet validation and packet verification. seDrip protocol, in data modeling part, the network mentors gets their asymmetric and symmetric keys, and then place the public arguments on each mote before the network deployment. In user enter part, a user gets the disseminated data authorize through registering to the network mentors. In packet validation part, a user registered and wants to dissemination some data, they required to create the data dissemination packets and then send them to the mote. In packet verification part, a mote verifies every accepted packet. If the result is positive, it updates the data related to the accepted packet. After a wireless sensor network (WSN) is utilized, there is normally required to update old small programs or parameters stored in the mote. This could be carry out by seDrip, which request a source to insert small codes, commands, controls, and configuration fields to mote. For modifying configuration arguments distributing management commands, data dissemination protocol is important.

A.Simulation Design Model



NAM - The Network Animator

Welcome to Nam 1.0a11a

Developed by UCB and the VINT, SAMAN, and Conser projects at ISI.

Nam contains source code with the following copyrights:

Copyright (c) 1991-1994 Regents of the University of California.
Copyright (c) 1997-1999 University of Southern California
Copyright (c) 2000-2002 USC/Information Sciences Institute

Fig 3: Network model

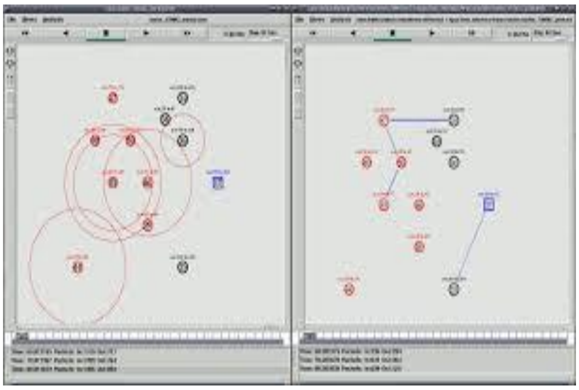


Fig 4: Secure data dissemination

X.CONCLUSION AND FUTURE WORK

This paper proposed the data dissemination protocol for distributed data in wireless sensor networks. This addresses the drawbacks associated with sink based approach of data dissemination. Also the security problems which were the main faults to be concerned in earlier approaches are addressed here. This paper provides data authentication by a secure hash function.Data integrity is provided using RSA asymmetric algorithm which is a strong encryption technique. As a future enhancement, additional security measures like data confidentiality can be added and efforts are taken to reduce the memory and energy overheads.

REFERENCES

[1]. He D, Chen C, Chan S, Bu J. DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks. Wireless Communications, IEEE Transactions on 2012; 11(5): 1946-1956.

[2]. Perrig A, Canetti R, Tygar JD, Song, D. Efficient authentication and signing of multicast streams over lossy channels. Security and Privacy, 2000.S&P 2000.Proceedings. 2000 IEEE Symposium on 2000;.56-73.

[3]. Levi A, Savas E. Performance evaluation of public-key cryptosystem operations in WTLS protocol. Computers and Communication.(ISCC 2003).Proceedings. Eighth IEEE International Symposium on 2003; 2: 1245-1250.

[4]. Sun Z, Ma Y. Copyright protection of multimedia content using homomorphic public key cryptosystems. Communications and Networking in China. ChinaCOM 2009. Fourth International Conference on 2009; 1-4.

[5]. Rahman M, El-Khatib K. Secure Time Synchronization for Wireless Sensor Networks Based on Bilinear Pairing Functions. Parallel and Distributed Systems, IEEE Transactions on 2010; 99: 1.

[6]. He D, Chan S, Tang S, Guizani M. Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks. Wireless Communications, IEEE Transactions on 2013; 12(9): 4638-4646.

[7]. Ceriotti M, Mottola L, Picco GP, Murphy AL, Guna S, Corra M, Pozzi M, Zonta D, Zanon P. Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment. Information Processing in Sensor Networks. International Conference on 2009; 277- 288.

[8]. He D, Chen C, Chan S, Bu J. DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks. Wireless Communications, IEEE Transactions on 2012; 11(5): 1946-1956.

[9]. Tolle G, Culler D. Design of an application-cooperative management system for wireless sensor networks, Wireless Sensor Networks 2005.

[10]. M. Kowsigan, P. Balasubramanie, An Improved Job Scheduling in Cloud Environment using Auto-Associative-Memory Network, Asian Journal of Research in Social Sciences and Humanities, Vol. 6, No. 12, December 2016, pp. 390-410.

[11]. M. Kowsigan, P Balasubramanie, Scheduling of Jobs in Cloud Environment using Soft Computing Techniques, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.38 (2015).

[12]. A. Jameer Baasha, R. Kanmani, Performance Analysis of Wireless OCDMA Systems Using PC OOC, EPC Codes, Asian Journal of Information Technology, Vol 15, No.12, pp.2087-20938.

[13]. A Jameer Basha, V Palanisamy, T Purusothaman, Multimodal Personal Authentication with Fingerprint, Speech and

Teeth Traits using SVM Classifier, European Journal of Scientific Research, Vol.6, No. 3, pp.463-473.

[14]. M. Kowsigan, S. Rajkumar, P. Seenivasan, C. Vikramkumar, An Enhanced Job Scheduling in Cloud Environment using Improved Metaheuristic Approach, International Journal of Engineering Research & Technology, Vol.6. No. 2, 2017

[15]. Lavanya. G, Pandeeswari. S, Shanmugapriya. R.K, Fuzzy Bases Interference Reduction in Cognitive Networks, International conference on advances in computing, Vol. 174, pp 1061- 1068, (2012).