ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Data Aggregation Using RSA Key Management Technique in Wireless Sensor Networks

C.Krishnan[1], Mrs.G.Malathy[2]

PG Student, Department of CSE, K S R Institute for Engineering and Technology, Tiruchengode, Tamil Nadu, India[1]

Associate Professor, Department of CSE, K S R Institute for Engineering and Technology, Tiruchengode, Tamil Nadu, India[2]

Abstract — Data sampled by sensor nodes having much redundancy. Data aggregation becomes an effective method to eliminate redundancy and minimize the number of transmission and then to save energy. To aggregate data by using ANT COLONY algorithm. Like Ant, it simply collects all the node information and sends to the destination. The ants to explore paths and follow the best paths with some probability in proportion to the intensity of the pheromone trail. In this the Data aggregation scheme employ Dynamic routing protocols and can forward packets(assigning attributes) with key security and time to time key value change dynamically by using RSA algorithm. The resources especially energy in wireless sensor networks (WSNs) are quite limited. Many applications can be deployed in WSNs and various sensors are embedded in nodes, the packets generated by heterogeneous sensors or different applications have different attributes. Most data aggregation schemes employ static routing protocols, which cannot dynamically or intentionally forward packets according to network state or packet types. To make data aggregation more efficient, proposed method using a RSA algorithm to implement a key based data transmission on network. The data's are aggregated using ant colony, a potential-based dynamic routing is elaborated to support and therefore improve the efficiency of data aggregation. The proposed work is to send the packets through secure routing and time to time key value change dynamically.

Key Words—Wireless sensor network, data aggregation, attribute-aware, dynamic routing, Security

I. INTRODUCTION

Wireless sensor networks (WSNs) are rapidly emerging technology which will have a strong impact on research and will become an integral part of future. The huge application space of WSNs covers national security, surveillance, military, health care, environment monitoring and many more.A WSN consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.Therefore, the primary challenge for this energy- constrained system is to design energy-efficient protocols to maximize the lifetime of the network. Wireless sensor networks are energy-limited and application specific. These two characteristics pose new challenges in the network design. Inch-scale sensor devices are expected to operate over years with limited power supply. Thus, the energy consumption becomes the foremost design consideration, while other constraints, such as throughput, latency, and fairness, become relatively less important. On the one hand, sensor networks are considered for a diverse range of civil and military applications, such as environmental monitoring, home networking, medical vital-signs monitoring, and smart battlefield, among others.

II. RELATED WORK

Data aggregation can be broadly classified into temporal and spatial solutions. The user makes packets more temporally convergent and the latter makes packets more spatially convergent. Next, the related work in these two aspects will be introduced. As for timing control scheme, TAG proposes a simple SQL-like declarative language for expressing aggregation queries over streaming sensor data and identifies the key properties of aggregation functions which affect whether data aggregations can be efficiently processed at some extent.

Next it focuses on designing a proper routing protocol for data aggregation. The sensor nodes are organized into clusters, a chain or a tree. In cluster-based solutions, each cluster has a designated sensor node as the cluster head, which aggregates data from all sensors

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

in the cluster and directly transmits concise digest to the sink. LEACH and HEED are two typical examples. The difference between them is the method of selecting cluster heads. LEACH assumes that all nodes have the same amount of energy capacity in each election round, while HEED aims to form efficient clusters to maximize network lifetime.

In a CWSN, sensor nodes are grouped into clusters, and each cluster has a cluster-head (CH)sensor node, which is elected autonomously. Leaf (non-CH)sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, we assume that, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained.

III. EXISTING SYSTEM

The concept of packet attribute, is used to identify the packets from different applications according to specific requirements can be identified. ADA (Attribute-Aware Data Aggregation) scheme uses PBDR (Potential Based Dynamic Routing) which can make the packets by using attributes for easily identifying. The sink resides at the bottom, and all packets in most of existing tree-based data aggregation schemes flow down along the surface directly just like water does without interacting with each other.

A. Disadvantages

- The sink nodes drop packets while aggregating
- The sensor nodes loss energy
- The packets from different application cannot aggregated(overlap)
- The user may have loss of time.
- saves only a limited energy in network life time.

B. Routing with Potentials

The PB-routing paradigm defines a scalar field on the network over which packets are routed. The potential at any node v is a function of and the destination d for which we need to find a route. More formally, with each node v (and destination d), we associate a potential that is single-valued. Note that if the destination d changes, the potential function for v changes as well. We prove all the properties of PB-routing assuming that the destination d is fixed. Since the potential functions for different destinations are independently defined, it follows that our assumption about a fixed destination is not restrictive.

For the rest of this paper, we shall use V (v) to denote the potential at a node v when the destination is clear from the context. Now consider a packet at p a node v host destination is node d. In order to reach d, p must be forwarded to one of the Z(v) neighbors of v. To determine this "next hop" neighbor, we define a "force" on the packet p at v based on the potentials at v and its neighbors. For a neighbor w ε nbr(v), we can define the force $F_{v\to w}$ as the discrete derivative of V with respect to the link metric as

$$F_{v\to w} = \frac{(V(v) - V(w)}{C_{v\ w}}$$

The packet p is now directed to the neighbor x ε nbr(v) for which the force $F_{v\to x}$ is maximum and positive. In other words, each packet follows the direction of the steepest gradient downhill to reach its destination. We now prove the following general property of the PB-routing paradigm.

IV. PROPOSED SYSTEM

A cryptographic algorithm is mainly used-RSA. By using this, the data packets are transferred through dynamic routing by time to time key value change securely.RSA implements two important ideas: Public-key encryption and Private-key decryption. In RSA, encryption keys are public, while the decryption keys are not. The person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. Through this process efficient data aggregation is achieved and the life time of sensor node is increased.

A. Advantage

- There is improvement in the efficiency of data aggregation
- The loss of data packets is reduced.
- The aggregated delay time is reduced.

B. Secure Data Aggregation

Like any other wireless sensor network protocol, data aggregation protocols must satisfy the security requirements explained in Section 2. However, the resource constrained sensor nodes and necessity of plain data for aggregation process pose great challenges when implementing security and data aggregation together. Security requirements of wireless sensor networks can be satisfied using either symmetric key or asymmetric key cryptography.Hence, the necessity of implementing the data aggregation and security using symmetric key cryptography algorithms have led many researchers to work on secure data aggregation problem.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

C. RSA Works and Use

- each user generates a public/private key pair by:

1. selecting two large primes at random - p, q (secret)
2. computing their system modulus N=p.q (public)
   - note ø(N)=(p-1)(q-1) (secret)
3. selecting at random the encryption key e (public)
   - where 1<e<ø(N), gcd(e,ø(N))=1
4. solve following equation to find decryption key d (secret)
   - e.d=1 mod ø(N) and 0≤d≤N
   - Use the extended Euclid's algorithm to find the multiplicative inverse of e (mod ø(N))

- publish their public encryption key: KU={e,N}
- keep secret private decryption key: KR={d,p,q}.
- Each block is represented as an integer number
- Each block has a value M less than N
- The block size is <= $\log_2(N)$ bits
- If the block size is k bits then
- $2^k <= N <= 2^{K+1}$
- to encrypt a message M the sender:
- obtains public key of recipient KU={e,N}
- computes: $C=M^e \bmod N$, where 0≤M<N
- to decrypt the ciphertext C the owner:
- uses their private key KR={d,p,q}
- computes: $M=C^d \bmod N$
- note that the message M must be smaller than the modulus N (block if needed)
- because of Euler's Theorem:
- $a^{ø(n)} \bmod N = 1$
- where gcd(a,N)=1
- in RSA have:
- N=p.q
- ø(N)=(p-1)(q-1)
- carefully chosen e & d to be inverses mod ø(N)
- hence e.d=1+k.ø(N) for some k
- Two cases:
- 1. gcd(M, N) = 1
- 2. gcd(M, N) > 1,

V. SYSTEM MODULES

A. Wireless Network Configures Setting

Wireless Sensor Networks create a number of nodes. The packets to send and receiving through the destination. It's based the scheme of packets delivered for ACK packet drop on the nodes. In this network to creating a sce to destination, intermediately set a server or base station on network. Transmit the data processing on whole networking.

B. Topology Design

This module is developed to Topology design all node place particular distance. Without using any cables then fully wireless equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The sink is at the center of the circular sensing area. Intermediate the sender and receiver of this networking performance on this topology.

C. Node Creating

This module is developed to node creation and more than 10 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

D. Mobile Relay Configuration

The mobile relay node act's as dynamic sensor node which moves around the sensor network. When it is revolve around the particular region, it emits the beacon message to its transmission range in the sensor network. Depends on the network size the number of mobile relay node is configured.

E. Data Aggregation Process

The sensor nodes, when receives the beacon messages, the sensor nodes of the particular region starts to sends the collected information. Based on the sequence time and priority of data packets transformation the packets are aggregated in the sink node. The packets are transformed to mobile sink node through the intermediate relay node.

F. Graph Design Based Result

Graph is an essential part of display a result, so plot a graph to show a various result comparison with packets, throughput, delivery ratio, network delay, energy consumption and etc.

VI. TOOL DESCRIPTION

Motivation for Simulation

- Cheap does not require costly equipment
- Complex scenarios can be easily tested
- Results can be quickly obtained – more ideas can be tested in a smaller timeframe

- The real thing is not yet available
- Controlled experimental conditions
- Repeatability helps aid debugging

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Features of NS-2

- Protocols: TCP, UDP, HTTP, Routing algorithms, MAC etc
- Traffic Models: CBR, VBR, Web etc
- Error Models: Uniform, bursty etc
- Misc: Radio propagation, Mobility models , Energy Models
- Topology Generation tools, Visualization tools and Tracing

Network Simulator Structure

- NS is an object oriented discrete event simulator
  Simulator maintains list of events and executes one event after another.
  Single thread of control: no locking or race conditions
- Back end is C++ event scheduler
  Protocols mostly and fast to run, more control
- Front end is oTCL
  Creating scenarios, extensions to C++ protocols, Fast to write and change
- C++: Detailed protocol simulations require systems programming language
  Byte manipulation, packet processing, algorithm implementation and Run time speed is important.

Turnaround time (run simulation, find bug, fix bug, recompile, re-run) is slower.

- Tcl: Simulation of slightly varying parameters or configurations

VII. CONCLUSION

The data's are aggregated by using Ant Colony algorithm and by providing key security to the packets dynamically with time to time key value change. It is an effective mechanism to save energy and provide security in WSNs.Packet loss will be reduced by using this technique. Transfer of packets will be increased in sensor networks. Duplication will be avoided. The secured data aggregation can be viewed only by the authorized persons. By using this, the data packets are transferred through dynamic routing by time to time key value change securely. RSA implements two important ideas: Public-key encryption and Private-key decryption. In RSA, encryption keys are public, while the decryption keys are private.

The person with the correct decryption key can decipher an encrypted message and the information can be viewed only by the particular person. Everyone has their own encryption and decryption keys. Through this process efficient data aggregation is achieved and the life time of sensor node is increased.

REFERENCES

1. Attribute-Aware Data Aggregation Using Potential-Based Dynamic Routing in Wireless Sensor Networks. Fengyuan Ren, Member, IEEE, Jiao Zhang, Yongwei Wu, Tao He, Canfeng Chen, and Chuang Lin,(2013) Senior Member, IEEE Vol. 24,no. 5
2. Acharya, M., & Girao, J. (2005). Secure Comparison Of Encrypted Data In Wireless Sensor Networks. In 3rd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, And WirelessNetworks (Pp. 47–53).
3. Basu, A. Lin, A. and Ramanathan, S. (2003) 'Routing UsingPotentials: A Dynamic Traffic-Aware Routing Algorithm', Proc.ACM SIGCOMM, pp. 37-48.
4. Lindsey S., C. Raghavendra, and K.M. Sivalingam "Data gatheringalgorithms in sensor networks using energy metrics (2002)
5. Mihir Bellare and Bennet Yee. Forward Security in Private Key Cryptography. Report 2001/035, Cryptology Eprint Archive, 2001.
6. Przydatek B., D. Song, and A. Perrig, "SIA: Secure Information Aggregation In SensorNetworks," In ACM Sensys, 2003, Pp.255–265.
7. Shih-I Huang Shiuhpyng Shieh J. D. Tygar Przydatek B., D. Song, and A. Perrig, "SIA: Secure Information Aggregation In Sensor Networks," In ACM Sensys, 2003, Pp.255–265.
8. Shih-I Huang Shiuhpyng Shieh J. D. Tygar (2010) Secure Encrypted-Data Aggregation For Wireless Sensor Networks.