ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 3, Issue 5, May 2014*

# Implementation of Trustable Routing Framework for WSNs

**Rutul S. Sanghavi[1], Nilesh R. Lendghar[2], Deepak S. Khade[3], Soumitra S. Das[4]**

Department of Computer Engineering, K J College of Engineering and Management Research, Pune, India[1,2,3,4]

**Abstract:** Recently use of Wireless Sensor Network Becomes Greater; there is little protection in Wireless sensor Networks (WSNs). In WSN the multi-hop routing against identity misdirecting through replaying routing information is also not secure. An Attacker can exploit this flow to launch various harmful or even destructive attacks against the routing protocols, like sinkhole attacks, wormhole attacks and Sybil attacks. The situation is further critical by mobile and harsh network conditions. Earlier cryptographic techniques or efforts at developing trustable routing protocols do not effectively address this severe problem. To secure the WSNs against attacker misdirecting multi-hop routing, we have designed and implemented Trustable Routing Framework for WSN, TRF provides trustworthy and energy-efficient route. Most importantly, TRF proves effective against those harmful attacks developed out of identity deceptions; the resilience of TRF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions. Further, we are implementing a low-overhead TRF module in Tiny OS. This implementation can be incorporated into existing routing protocols with the least effort.

**Keywords:** Wireless Sensor Network (WSN), Trustable Routing Framework (TRF)

## I. INTRODUCTION

Wireless Sensor Networks (WSN) [2] is a hybrid type of wireless network where data sensed by the sensors is not collected continuously by the sink. Data has to be secured by every node until the next visit of the mobile sink. This inability to communicate with sink might be for reasons such as: power constraints, limited transmission ranges or signal propagation problems. The concept of WSNs with a mobile sink looks realistic if we consider the environments where the sensing field is too far from the base station and sending data through intermediate nodes may result in weakening the security (e.g., intermediate nodes may modify the data) or increase the energy consumption[3] of the nodes close to the base station. In normal multi-hop WSNs, power [10] of the nodes placed near the sink will be exhaust before than the other nodes. This is because all the nodes have to transmit the data to the sink through the nodes placed near the sink. An WSN can be used to save the battery of these nodes and as a result increase the lifetime of the network Unattended environments as mentioned in include sensor networks for monitoring sound and vibration produced by troop movement, airborne sensor networks for tracking enemy aircrafts, LAN droids which retain information until soldiers move close to the network, Wireless sensor networks for monitoring nuclear excretions, national parks for discharge and illicit cultivation, etc. In many real world applications, critical-sensed data is collected and stored in the unattended nodes in hostile environments. Until the next visit of the sink the data should be accumulated. The unattended nature of the network and the lack of tamper resistant hardware increase the susceptibility of attacks over the data collected by the sensors. The sensors battery power is more limited compared to the battery power of the nodes in MANET's and hence the security protocols [4] for MANETs [5] are not effective for WSNs. Security needs should be taken into account to ensure data protection (also called data survivability) in these sensors at the time of design. Distributed security schemes are preferable over centralized schemes, because centralized schemes are prone to single point failure. Data security [7] and data authentication is a major concern in WSNs. Most cryptographic techniques [11] provide data authenticity and integrity but do not ensure data survivability [6]. This implies that if an enemy compromises a sensor and destroys the data contained therein, the data is lost permanently. The other drawback of cryptographic schemes is that they are computationally expensive for resource constrained sensor nodes. Due to these reasons, cryptographic techniques can be considered non cryptographic ones. In past few years, techniques for data authentication were proposed and cryptographic techniques for data protection were proposed. All these schemes assume that the sensors are static between successive visits from the sink.

However, this assumption is not practical in many real world applications and hence should be relaxed and allow nodes to move between two consecutive visits from the sink. Another important concern in WSN's is a mechanism is needed to ensure that the data received at the sink is authentic. The important objective of some of the adversaries is to inject fraudulent data into the information collected by the nodes and remain undetected. The mobile adversary is capable of compromising k out of n nodes in each round and it can also switch to different set of k nodes per round. Authentication schemes for WSN against a mobile adversary presented in and guarantee good security but suffer from high communication cost relative to the level of security achieved. Section II gives overview, Section III Brief Description, Section IV gives

Propose Solution, Section V gives Evaluation, Section VI gives Results and Section VII is Conclusion.

## II. OVERVIEW

TRF secures the multi hop routing in WSNs against intruders misdirecting the multi hop routing by evaluating the trustworthiness of neighbouring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. TRF is also highly scalable, energy efficient and well adaptable.

For a TRF-enabled node N to route a data packet to the base station, N only needs to decide to which neighbouring node it should forward the data packet considering energy efficiency and the trustworthiness. Once the data packet is forwarded to that next-hop node, the next task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decision its next-hop node makes. N maintains a neighbourhood table with trust level values and energy cost values for certain known neighbours. It is sometimes necessary to delete some neighbours' entries to keep the table size acceptable. In TRF, in addition to data packet transmission there are two ways of routing information: from the base station broadcast messages about data delivery and energy cost report messages from all nodes. This message needs acknowledgment. A broadcast message from the base station is flooded to the whole network. Its field of source sequence number is checked to evaluate freshness of a broadcast message. The other type of exchanged routing information is the energy cost report message from each node, which is broadcast to only its neighbours. Any node receiving such an energy cost report message will not forward it.

For each node N in a WSN, to maintain such a neighbourhood table with trust level values and energy cost values for certain known neighbours, two components, Energy Watcher and Trust Manager, run on the node. Energy Watcher is responsible for recording the energy cost for each known neighbour, based on N's observation of one hop transmission to reach its neighbours and the energy cost report from those neighbours. A compromised node may falsely report an extremely low energy cost to lure its neighbours into selecting this compromised node as their next-hop node; however, these TRF-enabled neighbours eventually abandon that compromised next-hop node based on its low trustworthiness as tracked by Trust Manager.

Encryption can also be used to protect the data but it involves certain non-negligible costs such as key management and computation involved to perform the encryption. Asymmetric cryptography is considered as a good choice for sensors. Using encryption, nodes can hide the data such that the adversary cannot identify a specific data. Identity of the nodes that collected the data can also be hidden using encryption. However, encryption cannot be considered as an option if the goal of the adversary is to completely erase the data in the node, and in case of public key encryption, sink has a public key which n is known to all the nodes. Nodes after collecting the data, encrypts the data using the sink's public key. To decrypt this sink's decryption key should be used. In this case, it is difficult for the adversary to detect the target data. Adversary can try to detect the target data by encrypting a sample data using sink's public key, the target data can also be replaced by different data since the adversary has the knowledge of the public key. To avoid this one-time random number can be used along with the public key to encrypt the data. This way it is not feasible for the adversary to distinguish the encrypted data.

### A. *Existing System:*

The presence of active adversaries suggests improving key management through the introduction of distributed healing schemes. Homomorphic encryption can be used to enhance storage and transmission efficiency. Data replication and replica dissemination can provide data survivability and integrity. Unfortunately, replication undermines data confidentiality, and replica diffusion via independent RWs in a static network exposes source-location privacy. Assuming that the sink can access a much larger fraction of the network than any realistic adversary, it is propose threshold secret sharing to get the advantages of replication without compromising data confidentiality.

## III. BRIEF DESCRIPTION

The main idea of this system is to provide a more security to the Wireless sensor network; and develop a robust trustable routing framework for dynamic WSNs. TRF provides trustworthy and energy-efficient route. The resilience of TRF is varied through extensive evaluation with both simulation and empirical experiments on large-scale in order to provide a heavy data authentication. By extending the team protocol we can provide a secure data authentication even in the presence of adversary attackers. While dealing with WSNs security [13] [14], the main focus is on achieving some or all of the following security goals:

*A. Forward Security:* The compromise of a secret in one round should not lead to the compromise of the secrets in the rounds preceding compromise. Forward security is critical in WSNs so that even if the adversary can compromise the current key it is infeasible for it to generate the previous keys using the current key. The adversary cannot even forge the authentication tags for the data generated and authenticated before compromise.

*B. Backward Security*: The compromise of a secret at any time should not lead to the compromise of the secrets to be used in the future. An adversary cannot decrypt the data generated and encrypted after compromise, if an adversary obtains the current status of the node. Adversary should not able to forge the authentication tags for the data generated and authenticated after compromise.

*C. Data Confidentiality:* Confidentiality ensures that the information is inaccessible to unauthorized users. In WSNs, data in the sensors should be encrypted in a way that it can only be read by the sink. In some scenarios, data from the nodes will not be sent to the sink in a single hop. Sink visits a point for data collection which can be few hops away from the node and the data has to be sent through other nodes. In these cases the intermediate nodes should not be able to read the transmitted information. Data confidentiality also prevents the read only adversary from reading the stored data in the compromised node's memory.

*D. Data Integrity:* Data integrity protects against unauthorized alteration of the data. Data integrity can be achieved only if the network has the ability to detect the manipulations done to the data by unauthorized parties, i.e., insertion, substitution and deletion.

*E. Data Authentication:* Authentication applies to both nodes and data. It ensures the identity of the node with which it is communicating i.e., the two communicating parties can identify each other. Information delivered through the network should be authenticated with respect to the generation time, date of origin, origin etc., and Data origin authentication also provides data integrity as the message modification can be detected.

## IV. PROPOSED SOLUTION

### *A. Proposed System*

We assume that the adversary can both eavesdrop the communications between any two nodes of the network and corrupt nodes to access all the data and key material they store. However, assuming the use of symmetric key encryption, the adversary can only read data received and stored by the corrupted nodes, for which it has access to the key. Observe that, if the amount of sensed, plaintext, data available to the adversary was the same available to the sink. An enhanced asymmetric cryptography algorithm in implemented to detect the sink hole attack and makes a secure and energy efficient communication in sensor network with the instant of trust manager and energy watcher. The proposed TRF provides a secure data transmission from sensor node to sink node.

### *B. Architecture*

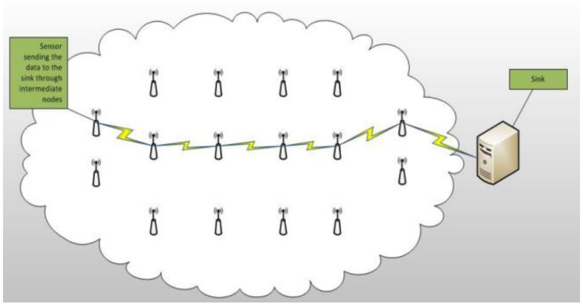

Sensor sending the data to the sink through intermediate nodes
Sink

Fig. 1 Architecture diagram of sensor nodes distribution, the sensor mode sends the sensed data to sink node through the intermediate nodes

### *C. Algorithm*

1) for neighbour discovery, (ndp-algorithm)
2) for key authentication-md5 cryptographic hashing algorithm

### *D. Implementation Environment*

Network simulator 2 is used as the simulation tool in this project. NS was chosen as the simulator partly because of the range of features it provides and partly because it has an open source code that can be modified and extended. There are different versions of NS and the latest version is ns-2.1b9a while ns-2.1b10 is under development

### *E. Experimental Setup*

In the simulation, 80 nodes are randomly distributed within a network field of size 1500mx300m as such a rectangle field can make the number of hops between two nodes larger. Mobile nodes are moving in the field according to the random way point model, and It adopt the speed ranges used in  so that the average speeds range from 0 to 10m/s. Two different CBR traffic loads are generated for each of the 20 pairs selected from the 50 nodes:2 packets/s as the light traffic load and 4 packets/s as the heavy traffic load. The local session keys are updated every 40 seconds in the simulation, and each update involves a complete anonymous key establishment procedure. To simulate cryptographic operations on each node, it forces each node to delay for some time according to the benchmarks. The period a node needs to wait is determined by cryptographic operations the node performs.

In TRF trusted neighbours will forward route packets for each other, otherwise packets are simply dropped, and identified particular node be malicious node Local key update and node mobility lead to trust lost batten one and its neighbours. Before neighbouring nodes establish shared local keys, no traffic can be passed between them, which results in transmission delay in existing mechanism. It evaluates the performance of enhanced TRF in terms of packet delivery ratio, packet delivery latency, and normalized control bytes. The proposed work demonstrates performance of  TRF at different moving speeds for two different traffic loads. Two traffic loads are selected according to performance of the standard implementation of ns2.

Ns-2 is a packet-level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration. Centric event scheduler cannot accurately emulate “events handled at the same time” in real world, that is, events are handled one by one. This is not a serious problem in most network simulations, because the events here are often transitory. Beyond the event scheduler, ns-2 implements a variety of network components and protocols. Notably, the wireless extension, derived from CMU Monarch Project, has 2 assumptions simplifying the physical world: Nodes do not move significantly over the length of time they transmit or receive a packet. This assumption holds only for mobile nodes of high-rate and low-speed. Consider a node with the sending rate of 10Kbps and moving speed of 10m/s, during its receiving a packet of 1500B, the node moves 12m. Thus, the surrounding can change significantly and cause reception failure. Node velocity is insignificant compared to the speed of light.

### *F. Modules description*

*a. Data Confidentiality*

Confidentiality ensures that the information is inaccessible to unauthorized users. In WSNs, data in the sensors should be encrypted in a way that it can only be read by the sink. In some scenarios, data from the nodes will not be sent to the sink in a single hop.

Sink visits a point for data collection which can be few hops away from the node and the data has to be sent through other nodes. In these cases the intermediate nodes should not be able to read the transmitted information. Data confidentiality also prevents the read only adversary from reading the stored data in the compromised node's memory.

*b. Data Integrity*

Data integrity protects against unauthorized alteration of the data. Data integrity can be achieved only if the network has the ability to detect the manipulations done to the data by unauthorized parties, i.e., insertion, substitution and deletion.

c. *Adversary detection*

The malicious nodes in the network are detected based on the trust level of the sensor node and also by key authentication mechanisms. The trust manager plays the vital role in establishing trust level of the node which is also used to transmit data through energy efficient nodes.

*d. Data Authentication*

Authentication applies to both nodes and data. It ensures the identity of the node with which it is communicating i.e., the two communicating parties can identify each other. Information delivered through the network should be authenticated with respect to the generation time, date of origin, origin etc., and Data origin authentication also provides data integrity as the message modification can be detected.

## V. EVALUATION

| | |
|---|---|
| Simulation Time | 100s |
| Scenario Dimension | 1500m x 300m |
| Wireless Radio Range | 250m |
| Mobile Nodes Number | 50 |
| Average Node Speed | 0-10m/s |
| Source-Destination Pairs | 20 random pairs |
| Traffic Type | 512-byteCBRtraffic |
| Traffic Frequency | 2 or 4 packets/s |
| Wireless Bandwidth | 2Mbps |
| Node Pause Time | 0s |
| Key Update Interval | 10s |
| Average Hops | 4 |
| Average Neighbours | 5 |

Table 1. Simulation Parameters

## VI. RESULTS

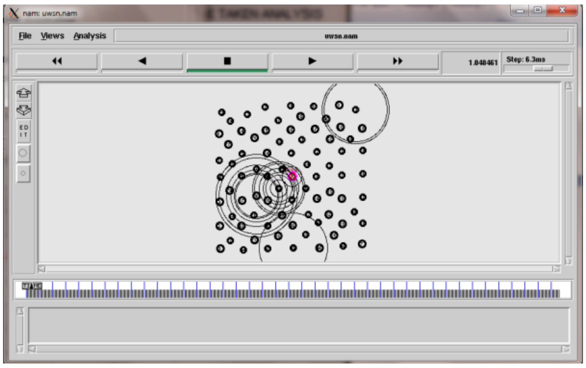
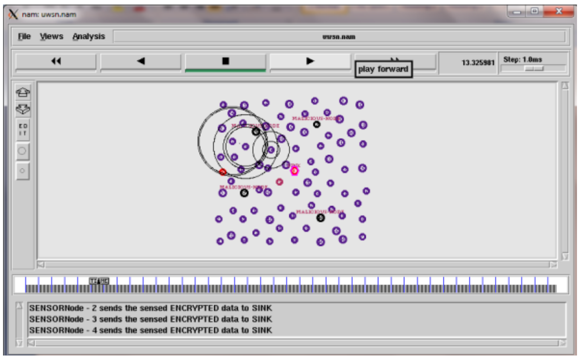


Fig.2.Sensor node creation in the sensor network, more than 50 sensor nodes created and distributed in the network.



```
SENSORNode - 2 sends the sensed ENCRYPTED data to SINK
SENSORNode - 3 sends the sensed ENCRYPTED data to SINK
SENSORNode - 4 sends the sensed ENCRYPTED data to SINK
```

Fig.3.Sensor node sends the encrypted data to sink through the intermediate nodes, through our cryptographic function the malicious nodes are detected.

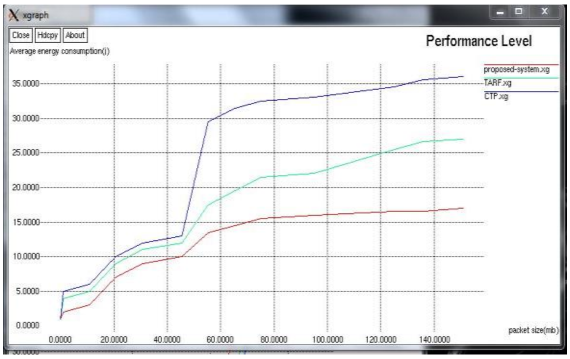


Fig. 4 Energy Consumption Graph.

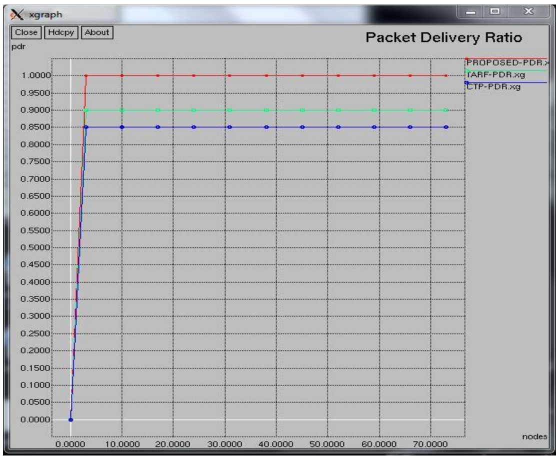


Fig. 5 Packet Delivery Ratio.

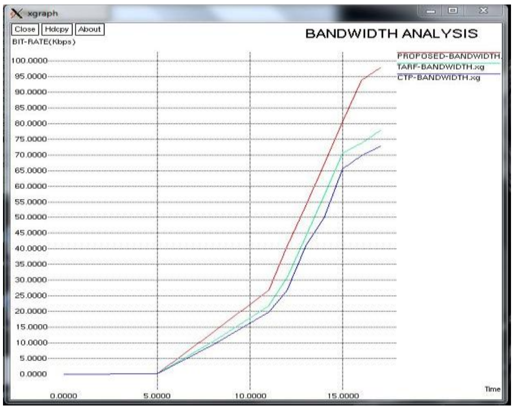


Fig6. Bandwidth Analysis.

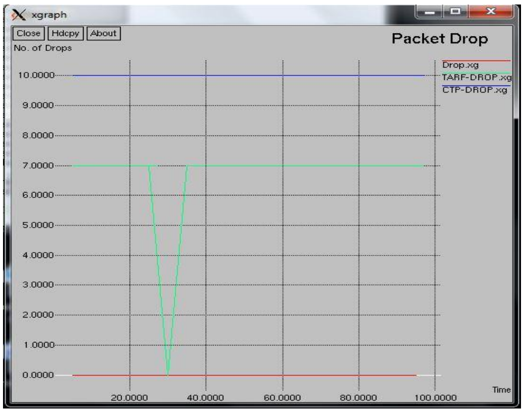


Fig7. Packet Drop.

## VII. CONCLUSION

We focused on information availability and confidentiality via secret sharing in WSN. We bounded the amount of information retrievable by the sink and by the adversary, as a function of the parameters k and n of the secret sharing scheme and of the accessed fraction of the network. We proposed enhanced asymmetric cryptographic schemes suitable for data protection against two types of adversaries with less communication and memory overhead and with a easy routing scheme. Our system can be used against proactive adversary, and performs well against reactive adversary.

## ACKNOWLEDGMENT

We would like to thank our guide for his guidance and support to complete this paper. We are thankful to our college for providing infrastructure, other facilities and also thankful to the principal for their constructive comments and suggestions.

## REFERENCES

[1] IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012Design and Implementation of TARF:A Trust-Aware Routing Framework for WSNs Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng F. Zhao and L. Guibas, Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, 2004.

[2] J. Al-Karaki and A. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” Wireless Comm., vol. 11, no.6, pp. 6-28, Dec. 2004

[3] J. Zhao, R. Govindan, and D. Estrin, “Computing aggregates for Monitoring sensor networks,” in Proc. 2nd Int. Workshop Sensor Network Protocols Applications, 2003.

[4] Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: A secure hop-by-hop data aggregation protocol for sensor networks,” in Proc. Seventh ACM Int. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc).

[5] J. Considine, F. Li, G. Kollios, and J. Byers, “Approximate aggregation techniques for sensor databases,” in Proc. IEEE Int. Conf. Data Engineering (ICDE), 2004.

[6] M. Garofalakis, J. M. Hellerstein, and P. Maniatis, “Proof sketches: Verifiable in-network aggregation,” in Proc. 23rd Int. Conf. Data Engineering (ICDE), 2007

[7] M. B. Greenwald and S. Khanna, “Power-conservative computation of order-statistics over sensor networks,” Proc. 23th SIGMOD Principles of Database Systems (PODS), 2004

[8] P. Flajolet and G. N. Martin, “Probabilistic counting algorithms for data base applications,” J. Computer Syst. Sci., vol. 31, no. 2, pp. 182–209,1985.

[9] M. B. Greenwald and S. Khanna, “Power-conservative computation of order-statistics over sensor networks,” Proc. 23th SIGMOD Principles of Database Systems (PODS), 2004.

[10] A. Liu and P. Ning, “Tinyecc: A Configurable Library forElliptic Curve Cryptography in Wireless Sensor Networks, ”Proc. Seventh Int’l Conf. Information Processing in Sensor Networks (IPSN ’08), pp. 245-256, 2008

[11] J. Al-Karaki and A. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” Wireless Comm., vol. 11, no. 6, pp. 6- 28, Dec. 2004.

[12] H. Chan, A. Perrig, and D. Song, “Secure hierarchical in-network aggregation in sensor networks,” in Proc. ACM Conf. Computer and Communications Security (CCS), 2006.

[13] K. B. Frikken and J. A. Dougherty, “An efficient integrity-preserving scheme for hierarchical sensor aggregation,” in Proc. 1st ACM Conf.Wireless Network Security (WiSec), 2008.