International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

Privacy Preservation Scheme for WSNs using Signature and Trust Value Computation

Pavithra M. N
PG Student,
Department of IS&E
National institute of Engineering,
Mysore, Karnataka, India

Chinnaswamy C. N
Associate Professor,
Dept. of IS&E
National Institute of Engineering,
Mysore, Karnataka, India

Dr. T. H. Sreenivas
Professor,
Dept. of IS&E
National Institute of Engineering,
Mysore, Karnataka, India

***Abstract* - A WSN are spatially distributed sensor nodes that monitor physical or environmental conditions such as fire detection, habitat monitoring, and traffic management, battlefield surveillance, which has limited power, computation, storage and communication capacities. Nowadays more and more WSNs are implemented in different areas so high privacy is required in both context and data. To preserve privacy of wireless sensor network use various techniques. Trust management systems could play an important role to preserving privacy in WSN which also enhance the reliability and security of WSN. In trust management, computing trust value is one of the crucial problems. In this scheme we compute trust value for each sensor node for preserving privacy of data. Sensor node uses secure message distributed with configurable privacy with secure delivering centre. Secure delivering centre sends different messages to different users with same signature based on trusted routing path (trust value). The user can only known the message intended for him, at same time every user can verify the signature. It is resilient against the node internal and external attacks.**

Key Words:* *Trust management, privacy preserving data, Trust value, trust path, signature, TARF, MD5 with RSA.

I. INTRODUCTION

A wireless sensing element network is a distributed system consists of varied sensor nodes deployed in environments to sense the physical world. Wireless sensor networks have a large number of applications, such as battle field surveillance, environment monitor, personal health monitor, They experiences from limited computation, communication, and power resources and so on. WSNs have the attractive features and the progressively important roles, sensor networks but have their inherent restrictions. Sensors are usually resource-limited and power-constrained. They experience the ill effect from restricted computation, communication, and power resources. In many applications, WSNs are deployed in hostile environments that it is the higher possibilities for an adversary to attack the sensor node by physically compromising it. So the traditional cryptographic and authentication mechanisms alone are insufficient to protect WSNs.

The trust management system is one of the security mechanism, which is construct a self-healing ,tries to avoid insider attacks in WSNs and it naturally executes the procedure of figuring out if access ought to be permitted by particular strategy, access rights and approval semantics.

The reason of trust model is to construct trust mechanism for every node inside network. The model assesses node communication behaviour, estimate trust value of nodes, which give metric to the model can recognize suspect nodes inside network and decrease their impaction to information procurement and communication in greatest degree. Trust is an essential part of decision making for the distributed computing applications. The important of trust is represented by the labelled transition systems and the immediate trust level can be calculated by the testing pre orders. Its significant shortcoming is that it cannot be ensured that clients will precisely assign values appropriately.

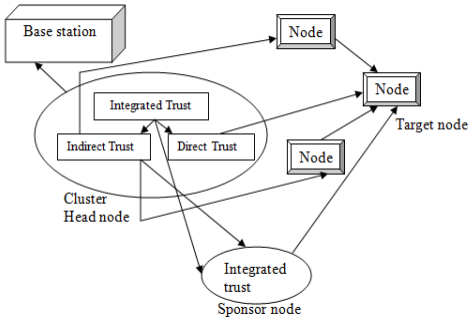


Fig 1 storing direct and indirect trust value in all nodes

As shown in Figure 1, every node stores all the immediate (direct) trust values of every other node in the same cluster, every node then sends all the immediate trust estimations of different nodes to the cluster head. Utilizing the immediate trust values the cluster head figures and stores the indirect (group) trust data for every node in the cluster. Likewise, the cluster head additionally stores its own immediate trust value for every node as well as the energy level of every node living in its cluster. The cluster head then calculates the integrated trust value for every node in the cluster taking account the gathering and cluster head's immediate trust values.

Reputation or trust management system can be valuable for identifying a node which is maliciously or faulty (broken) and it can help in decision-making process. Individual suppositions of different nodes and are generally considered confidential. Be that as it may, past works give careful consideration to privacy preserving in the computation of trust value. Yao et al. suggested a distributed scalar product protocol with application to privacy-preserving

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

computation of trust value. In any case this protocol is based on homomorphic encryption computation, due to the computation restriction of WSNs, it is not appropriate for WSNs. In WSNs the traditional cryptographic mechanisms are insufficient when the control of sensor nodes is taken by an inside adversary. Trust management system can take care of this issue effectively, and improve the security and reliability of WSNs. Estimating the trust values of nodes is one of the key problems in trust management system. Be that as it may, past works give careful consideration to preserving data privacy during computing trust value.

A. Existing solution

Xing Yuan et al "Privacy Preserving Computation of Trust-value in Wireless Sensor Networks" [2] This paper concentrate on the issue that how to secure the data privacy while computing trust values, and proposes a privacy preserving trust value computation (PPTC) protocol to take care of the this issue. No need any encryption or decryption operations here. Disadvantages: The existing system suffers from security.

To overcome the above shortcomings, sensor node uses secure message distributed with configurable privacy with secure delivering centre. This proposes secure delivering centre sends different messages to different users with same signature based on trusted path (trust value). The user can only known the message intended for him, at same time every user can verify the signature. It is resilient against the node internal and external attacks.

The rest of paper is organized as follows: section 2 present the related work of the proposed scheme ,section 3 describe proposed solution ,section 4 explain the result in plotting graph , section 5 concludes.

II. RELATED WORK

In 1996 Blaze et al. (1996) firstly proposed a trust management system, called Policymaker, to determine and uphold security policy, credentials and connections that permit direct approval of basic security activities. Understood thoughts of trust are taken care of by applications which depend on cryptographic methods. A trusted third party signs a declaration message to guarantee the identity connected with a public key.

Xing Yuan et al [2] explain how to ensure the information privacy while computing trust values, and propose a privacy preserving trust value computation (PPTC) protocol to take care of this issue. Utilizing private distributed scalar product protocol taking into account semi-honest third party to accomplish the PPTC protocol. In this approach the attackers are divided into two kinds: semi-honest attackers and malicious attackers. The Agent is assumed to be semi honest, and is trusted by all the sensor nodes. So the agent is also required high security and computation power, but wireless sensor network are limited resources, power constraints.

In 2007, Yao et al. [4] proposed a distributed scalar product protocol with application to privacy preserving computation of trust. This protocol is split in two phases: a homographic encryption computation; and a private multi-party summation protocol. The protocol has two drawbacks: a) It generates a non-negligible communication overhead and b) It introduces a security flaw. The contribution of this paper is two-fold. First prove that the protocol of is insecure in the semi-honest model by demonstrating that it is not opposing to collusion attacks and we give an case of a collusion attack, with only four participator. Second, It propose to use a superposed sending round as an alternative to the multi-party summation protocol, which results in better security properties and in a decrease of the correspondence costs. Second, we exhibit another plan which opposes to collusions. It can be balanced for any application that requires a secure distributed scalar product for trust establishment, particularly, for suggestion and reputation systems.

YaHui Li et al [1] presented There is an SDC (Secure Delivering Centre) can be a trusty fixed sink node. The sensor node uses SMDCP (Secure Message Distribution Scheme with Configurable Privacy) with SDC. At this point, SDC decrypts the secret messages and verifies the signature. After this, in the view of a pre-set policy, SDC sends different messages to different various clients with all these messages the same signature. At the meantime, every client can confirm the signature. However, the sensor node can only generate one signature for all the messages for all the users if attacker fined that signature attackers can easily decrypt the message and also secure delivering centre is a fixed sink node so the location privacy required.

S.Ganeriwal et al [3] author proposed a reputation based framework for sensor networks where nodes keep up reputation for different nodes and use it to assess their reliability. In this paper author mentioned a framework, RFSN, for developing a community of trustworthy sensor nodes at runtime based upon the behaviour of these nodes. The lightweight modular architecture of RFSN has been designed keeping into mind the resource requirement nature of sensor nodes. Inside the framework of RFSN, they built up a beta reputation system for sensor networks (BRSN) that uses a Bayesian formulation for reputation representation, updates, integration and trust evolution. We have provided a detailed examination of our system design choices, standing out them from existing reputation-based systems from e-trade and ad-hoc networks.

D. Yao et al proposed [4] DRBTS is a distributed security protocol went for giving technique by which BNs can monitor each other and gives information so that SNs can pick who to trust, based on a majority voting approach. So as to trust a BN's information, a sensor must get votes for its reliability from at any rates half of their common neighbor.

In this paper author determine a private distributed scalar product protocol that can be used for getting trust values from private suggestions. Our protocol permits Alice to induce the reliability of Bob in view of what Alice's companions think about Bob, and Alice's confidence in her companions. Also, the private information of Alice and her companions are not revealed during the computation. The trust model is simple to compute, yet it is scalable as it classifies large groups of users. Reputation or trust models provide an open, flexible, and dynamic mechanism for trust establishment, where the requester does not be a part of the resource owner. Trust models have applications in distributed systems such as peer-to-peer networks, in resource-sharing systems such as Grid computing- commerce applications such as ebay.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

XIAO Mingjun et al [5] author applies the techniques of secure multi party computation (SMC) to solve the above-mentioned problem, and propose a PPHC protocol. This paper however introduces a data-level location privacy problem, i.e., the Privacy preserving hop- distance computation (PPHC) problem, in this protocol, the data disguise techniques in the secure multi-party computation field is successfully applied to protect the location privacy of each participant. The most advantage of this protocol is that it does not require any trusted third-party or encryption operations, and thus has a much better performance than the traditional solution generally based on a trusted third-party and encryption operations. The performance analysis shows that the computational overhead of this protocol is only O(1), and the communication over head is dominated by two rounds of message delivery.

Carlos Aguilar Melchor et al [6] proposed A Collusion-Resistant Distributed Scalar Product Protocol with Application to Privacy Preserving Computation of Trust in 2007 Yao et al. proposed a distributed scalar product protocol with application to privacy preserving computation of trust. This protocol is split in two phases: a homographic encryption computation; and a private multi-party summation protocol.

III. PROPOSED SOLUTION

In our approach we combine both trust value and signature computation for preserving privacy data. The trust estimation of sensor nodes is computed to guarantee whether the sensor node is a generous or malignant one. It is assessed from the historical scenery of exchanges with the node and from the suggestions given by other neighbour node inside system. At first, whenever a sensor node joins to network, it is assumed that the node N is a Trustworthy node i.e. some trust value will be allocated to the node depending upon the threshold trust value. At the point when the communication between node i and node j happens, node i will assess the trust value of node j, and afterward choose whether to collaborate or not.

The proposed solution consists of two parts:

1. Trust Value Computation and Exchange
2. Sending Different Secure Message with Same Signature

A. Trust Value Computation and Exchange

In this scheme for trust value computation and exchange we are using the TARF [7] [9] (trust aware routing frame-work) for WSN .A sensor node wirelessly sends a message to a base station via multi-hop path, TARF provide trustworthy and energy-efficiency route effective against harmful attack. Protect WSNs from harmful attacks exploiting the replay of routing information and it not tight time synchronization and known geographic information.

For calculating trust value and routing in TARF is first initialize source and destination node, for node N, a neighbor of node N's is reachable from N with one-hop wireless transmission. After routing finding, every node stores multiple routing paths to reach base station. Base station broadcasting messages all the nodes in the network to send data from one node to another node. For a node N, the trust level of the neighbor N's calculating of the probability that this neighbor accurately delivers data received to the base station. Initially it have some threshold trust value , the node will give mistrust reports to base station, if finding neighbour node trust value is lower than threshold value. If multiple node report same mistrust in many times the base station will exclude the node from routing table and its loop free. If N discovered that any received data packet is already in that record the packet will be discarded, and N also degrades trust value its next-hop. Energy cost will recording from energy watcher for every known neighbours ,node N one hop transmission to reach its neighbour based and cost of energy is reports those neighbours.

B. Sending Different Secure Message with Same Signature

In proposed scheme sending secure message from source to destination along with the trusted path we using MD5-RSA technique RSA is joined with the MD5 hashing function to sign a message in this signature suite. It must be infeasible for anybody to either discover a message that hashes to a given value or to discover two messages that hash to the same value. In the event that either was feasible, an interloper could join a false message onto Alice's signature. The hash functions MD5 has been composed particularly to have the property that finding a match is infeasible, and is along these lines considered appropriate for use in this role.

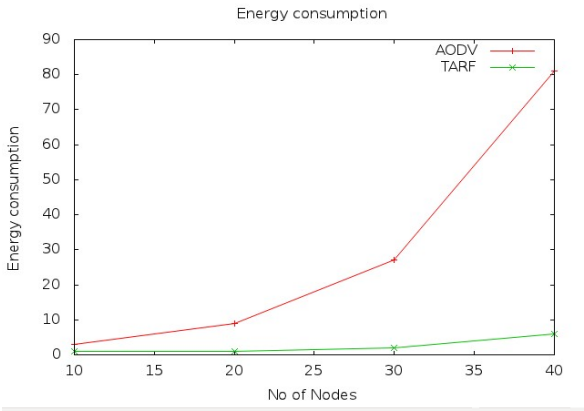
Steps involved in md5 with RSA

a. Initialize the RSA object with a RSA public key
b. Get message digest for all the data thus far updated, then sign the message digest.
c. Update digest with the passed in byte.
d. Update digest with an array of bytes.
e. Verify the signature (compare the result with the message digest).

TARFs to compute trust value, Exchange the trust value to its neighbour, and MD5 with RSA suit for forwarding secure message in secure delivering centre sends different messages to different users with same signature based on trusted path (trust value). The user can only known the message intended for him, at same time every user can verify the signature.

IV. RESULTS

We implemented the proposed solution in NS2 and measured the number of delivered packet, energy consumption, number of reported failure detection we compare obtained result into AODV routing protocol.



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

Chart -1: The energy consumption is more in AODV because it doesn't have any trusted path and all so it sends number of packets to its all neighbouring node that neighbouring node forward packet to all its neighbouring node so on. In our approach number of packet is forward only in most trusted path so it consume less energy.

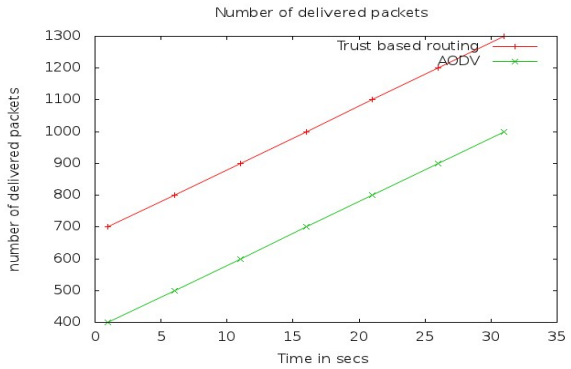


Chart -2: In over period of time the number delivered packet is more in our approach compare to AODV, initially it will be little as time progress it goes on increase because we are update more trusted path forwarding packet.

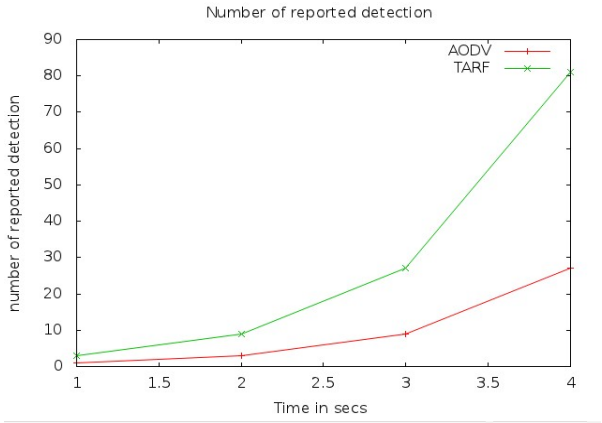


Chart -3: In compare to AODV, a number of node attacking is less in our approach.

V. CONCLUSION

In our approach, the trust value computing and sharing them with neighbors in distributed environment. Based on the trust value the secure delivering centre sends different messages to different users with same signature .It keep up reputation for each node and use it to evaluate their trustworthiness. Avoid inside and outside attack.

REFERENCES

[1] YaHui Li, DingYong, JianFeng Ma: Secure Message Distribution Scheme with Configurable Privacy for Heterogeneous Wireless Sensor Networks 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing

[2] Xing Yuan, Liusheng Huang and Wei Yang: Privacy Preserving Computation of Trust-value in Wireless Sensor Networks National High Performance Computing Center at Hefei, Department of Computer Science and Technology, China. 978-1-61284-486-2/111 2011 IEEE

[3] S.Ganeriwal, L.K. Balzano, and M.B. Srivastava. "Reputation-based Framework for High Integrity Sensor Networks" SASN'04, October 25, 2004, Washington, D.C., USA.

[4] D. Yao. R. Tamassia. And S.Proctor. "Private Distributed Scalar Product Protocol with Application to Privacy-Preserving Computation of Trust" Volume 238 of the series IFIP International Federation for Information Processing

[5] XIAO Mingjun, HUANG Liusheng, "Privacy Preserving Hop-distance Computation in Wireless Sensor Networks" Chinese Journal of Electronics Vol.19, No.1, Jan. 2010

[6] Carlos Aguilar Melchor, Boussad Ait-Salem "A Collusion-Resistant Distributed Scalar Product Protocol with Application to Privacy Preserving Computation of Trust" Conference Paper · August 2009

[7] Guoxing Zhan, Weisong Shi, and Julia Deng "TARF: A Trust-Aware Routing Framework for Wireless Sensor Networks" LNCS 5970, pp. 65–80, 2010.

[8] Youssef Gahi, Mouhcine Guennoun, Zouhair Guennoun, Khalil El-Khatib2 "An Encrypted Trust-Based Routing Protocol"

[9] M. Srikar Swamy G.S. Uday Kiran "Design and Implementation of TARF: A Trust–Aware Routing Framework WSN's" International Journal of Research Studies in Computer Science and Engineering (IJRSCSE) Volume 1, Issue 6, October 2014

[10] Shaik sahil babu, arnab raha, mrinal kanti naskar "A direct trust dependent link state routing protocol Using route trusts for wsns (dtlsrp)" wireless sensor network, 2011, 3, 125-134

[11] Swimpy Pahuja and Anita Singhrova "Preventive Alternate Path Routing Algorithm against Intrusion in Sensor Area Network" International Journal of Computer Theory and Engineering, Vol. 5, No. 2, April 2013

[12] Dr.S.Rajaram, A. Babu Karuppiah, K. Vinoth Kumar "secure routing path using trust values for wireless sensor networks" International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 2, June 2014