Design of Dependable, Trustworthy and Secure Communication in Wireless Sensor Network

Ashadevi.A[1] and RameshKumar.M[2]

[1]M.E CSE, Vel Tech Multi Tech Engineering College, Avadi, Chennai

[2]Asstprofesser, Department of Computer Science, Vel Tech Multi Tech Engineering College, Avadi, Chennai

Abstract

The clustered wireless sensor networks are incapable of satisfying the resource efficiency and trust system because of the high overhead and low dependability. A Light Weight and Dependable Trust System (LDTS) is used which employees the Clustering Algorithm. The nodes are registered in every network and the Cluster Head is identified based on the number of connections. Base Station acts as an Intermediate Node to Monitor the Data Transaction. The LDTS uses a self-adaptive feedback model for trust evaluation. Eventhough this enhances the energy efficiency and confirms the trustworthiness of nodes that participate in the communication, there are certain drawbacks. The trust values can be analyzed by an intruder and also there is no authentication for the messages being transmitted. The main characterestics of WSN's are their limited processing, storage, bandwidth and energy. After considering all these issues, in the proposed system, a lightweight simple and robust key generation algorithm is used. This algorithm provides authentication and security for trust messages as well as data messages and results in the design of an energy-efficient, trustworthy and secure communication model in wireless sensor networks.

Index Terms— *Self-adaptivite, trust system, RC4 Stream Cipher, Secure Protocol*

1. Introduction

Sensor networks contain hundreds or thousands of nodes, and they may need to be deployed in remote or dangerous environments, allowing users to extract information in ways that would not have been possible otherwise. Many clusteringalgorithms such as LEACH[1], EEHC[2], EC[3], and HEED[4] can effectively improve network scalability and throughput. Nodes are grouped into clusters, and within each cluster, a node with strong computing power or a node having close proximity to itsneighbours and base station(BS) is elected as a cluster head (CH). Usually the nodes closer to the sink will be heavily loaded. An Energy-Efficient Clustering (EC), determines suitable cluster sizes depending on the hop distance to the data sink, while achieving approximate equalization of node lifetimes and reduced energy consumption levels.Trust establishment in a clustered environment is of great importance. Trust is the expectation of one entity about the actions of another. A trust system enables a CH to detect faulty or malicious nodes within a cluster, guides the selection of trusted routing nodes through which a cluster member (CM) can send data to the CH. During intercluster communication, a trust system also aids in the selection of trusted routing gateway nodes or other trusted CHs through which the sender node will forward data to the base station (BS).

Motivation

A WSN comprises of battery-powered sensornodes with extremely limited processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multihop path. The resource efficiency and dependability of a trust system are the most fundamental requirements for WSNs. However, existing trust systems developed for clustered WSNs are incapable of satisfying these requirements because of their high overhead and low dependability.

Also, implementing complex trust evaluation algorithms at each CM or CH is not practical. In existing trust mechanisms, trust management systems collect remote feedback andthen the feedbacks from all the nodes are aggregated to obtain the global reputation which can be used to evaluate the globaltrust degree(GTD) of this node. Due to the broadcast nature of the WSN environment, it contains a large number of undependable (or malicious) nodes. Feedback from these undependable nodes may result in the incorrect evaluation of feedback.So a trust system should be highly dependable in terms of providing service in an open WSN environment.

Contributions

The main aim is to create a secure trust management system for clustered WSNs which enhances both dependability and resource efficiency. The new system go beyond existing approaches in terms of the following aspects:

1)A lightweight scheme for trust evaluation between CMs or between CHs.

Within the cluster, the CH evaluates the indirecttrust of its corresponding CMs. Therefore it is not necessary that each CM need to maintain the feedback from other CMs. This approach will reduce the communication overhead and eliminatethe illeffects of a bad-mouthing attack. The feedback of a CH is also obtained in the similar manner to obtain the same benefits.

2)A dependability-enhanced trust evaluating approach between CHs.

CHs takeon large amounts of data forwarding and communicationtasks. Taking this into consideration,a dependability-enhanced trust evaluating approachis defined for the communications between CHs. This approacheffectively reduces the networking consumption and thus prevents malicious, selfish, and faulty CHs.

3)A weighting method for CH's trust aggregation.

A self-adaptive weighting method is used which is different from the traditional methods. Weights are measured on the basis of trust factors rather than assigning subjectively.

4)A secure trust system using RC4 algorithm.

It is possible for an attacker to alter the trust values. Therefore it is necessary that the trust values should be passed secure. The data packets also needs to be encrypted during transmission so that theintermediate nodes are not able to view the data during transmission. For encryption process, considering the energy constraints of WSNs, a lightweight RC4 Algorithm is used.
These new designs and other specific features (e.g., independent of any specific routing scheme and platform and so forth) collectively makes the design a lightweight, self-adaptive, and dependable solution that can be used in any clustered WSN.

2. Related Work

Wireless sensor networks (wsns) are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. A number of such systems are proposed for WSNs [5], [6]--[8], [9], [10]. However, these systems have various limitations such as the incapability to meet the resource costraint requirements of the WSNs. Till now, there is no such trust system which has been successful in achieving dependability and resource efficiency in clustered WSNs.

Zhan, *et al.*[6] proposed a trust-aware routing framework for WSNs ,TARF which is a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient routing in WSN's. Also, TARF is very effective against the harmful attacks developed out of identity deception; the resilience of TARF 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.

Bao*et al.* [9] proposed HTMP, a hierarchical dynamic trust management protocol, to effectively deal with selfish or malicious nodes. Multidimensional trust attributes derivedfrom communication and social networks are considered to evaluate the overalltrust of a sensor node. A probability model utilizing stochastic Petri nets techniques is used to analyze the protocol performance, and validate subjective trust against objective trust obtained based on ground truth node status. Implementing such a complex trust evaluation scheme at each CM of the cluster is unrealistic.

Crosby et al. [11] proposed TCHEM, a distributed trust-based framework and a mechanism for the election of trustworthy cluster heads. This mechanism reduces the likelihood of compromisedor malicious nodes from being selected as cluster heads. TCHEM does not cover trust in detail, since numerous key issues of trust management are not introduced.

Yao et al. [10] proposed *PLUS*, a parameterized and localized trust management scheme for sensor networks security, where each sensor node maintains highly abstracted parameters, rates the trustworthiness of its interested neighbors to adopt appropriate cryptographic methods, identify the malicious nodes, and share the opinion locally**.**

Boukerche*et al.* [12] proposed ATRM,a novel agent-based trust and reputation management scheme (ATRM) for wireless sensor networks. Trust and reputation is suggested as an effective security mechanism for open environments such as the Internet, and considerable research has been done on modeling and managing trust and reputation. Using the trust and reputation management scheme to secure wireless sensor networks (WSNs) requires paying close attention to the incurred bandwidth and delay overhead, which have been focused by most research works. The objective of the scheme is to manage trust and reputation locally with minimal overhead in terms of extra messages and time delay. ATRM assumes that mobile agents are resilient against malicious nodes that try to steal or modify information such agents carry. In many applications, this assumption is unrealistic[13].

3 .System Model

A.Network Topology Model and Assumptions

First nodes are grouped into clusters and the cluster head is chosen. The cluster head is chosen based on the node having highest connectivity to all other nodes within the cluster or to the base station. So if the source wants to send the data to the destination node which is located in another network, first the data will be sent to the cluster head of the sender node's network. From that cluster head, the data will be passed to the cluster head of the destination node. Then the destination node's cluster head will re-send the data to the destination node via the best route.

Thus clustering effectively improves network scalability and energy-efficiency[15]. Therefore, in this model, nodes are grouped into clusters using an energy efficient clustering(EC) algorithm. This algorithm determines suitable clustersizesdepending on the hop distance to the data sink, while achieving approximate equalization of node lifetimes and reducedenergy consumption levels.

Algorithm 1

EC Algorithm**:**

```
Ensure: $T(K) \approx \ldots \approx T(i) \approx \ldots \approx T(1) \approx L$

$t \leftarrow 0$;
$P_t = P_0 = \{p_0, p_0, \ldots, p_0\}$;
$L_{t+1} \leftarrow L_0$;
$P_{t+1} = \{p_1, p_2, \ldots, p_K\} \leftarrow$ Calculate Ps($L_t$);
while $P_{t+1} = \{p_1, p_2, \ldots, p_K\}$ are Real and Non-negative do
    Determine $L_{t+1}$
    $P_{t+1} = \{p_1, p_2, \ldots, p_K\} \leftarrow$ Calculate Ps($L_{t+1}$);
    $P_t \leftarrow P_{t+1}$;
    $L_t \leftarrow L_{t+1}$;
    % An exit condition that meets a certain requirement specific to the protocol
    if $C(L_{t+1})$ = true then
        return $P_{t+1}$, $L_{t+1}$
    end if
    $t \leftarrow t + 1$;
end while
return $P_t$, $L_t$;
```

CalculatePs(L):

```
Solve $T(K) = L$ for $p_K$;
Solve $T(K - 1) = L$ with $p_K$ for $p_{K-1}$;
...
Solve $T(1) = L$ with $p_K, p_{K-1}, \ldots, p_2$ for $p_1$;
return $p_1, p_2, \ldots, p_k$;
```

The hot-spot issue is particularly significant around sink nodes where large amounts of data are merged. In fact, as the hop distance to a sink decreases, the load on relay nodes quickly intensifies. Hence, there is an obvious relationship between the hop-distance to a data sink and the amount of data that has to be relayed.

To obtain a well-balanced network load, this relation should be studied analytically. In doing so, the energy consumption of data communication and of control overhead caused by route discovery and any other procedures should be taken into account.

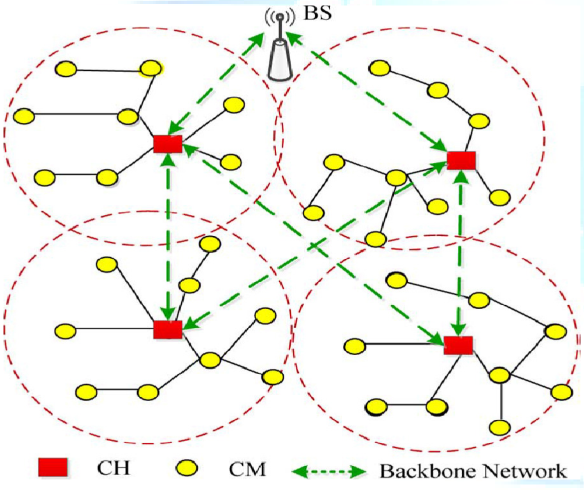

Fig. 1.Roles and identities of nodes in a clustered WSN model.

We propose a scalable, distributed, and energy-aware clustering algorithm, *Energy-efficient Clustering* (EC). EC determines suitable cluster sizes considering their hop distances to the data sink. By tuning the probability that a node becomes a CH, EC effectively controls cluster sizes, which allows an approximately uniform use of the overall energy resources of a WSN. However, EC is adaptable to any data delivery protocol used for data collection to a sink node.

B. Lightweight Scheme for Trust Decision-Making

LDTS(A lightweight and dependable trust system) facilitates trust decision-making based on a lightweight scheme.This scheme is described as follows:

1)Trust Decision-Making at CMLevel

A CM calculates the trust value of its neighbors based on two information sources (Fig. 2): direct observations (or direct trust degree, DTD) and indirect feedback (or indirect trust degree, ITD). DTD is evaluated by the number of successful and unsuccessful interactions. In this work, interaction refers to the cooperation of two CMs. All CMs communicate via a shared bidirectional wireless channel and operate in the promiscuous mode, that is, if node sends a message to CH via node, then node can hear wether node forwarded such message to CH , the destination. If does not overhear the retransmission of the packet within a threshold time from its neighboring node or if the overheard packet is found to be illegally fabricated, then willconsider the interaction unsuccessful. As an example of trust decision-making at the CM level, if a node wants to communicate with node , first checks whether it has any past interaction records with during a specific time interval. If a past interaction record exists, then makes a decision directly,Otherwise, will send a feedback request to its CH.

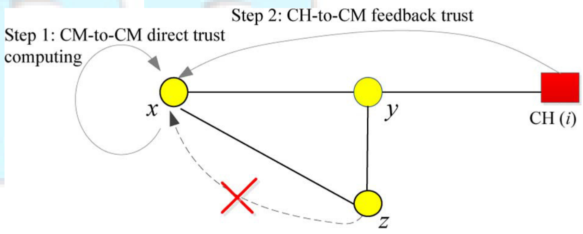
Step 2: CH-to-CM feedback trust
Step 1: CM-to-CM direct trust computing
x
y
z
CH (i)

Fig. 2. Trust decision-making at CM level.

2) Trust Decision-Making at CH Level

The selection of CHs is a very important step for dependable communication. In LDTS, the GTD of a

CH is evaluated by two information sources (Fig. 3): *CH-to-CH* direct trust and *BS-to-CH* feedback trust.

During *CH-to-CH* communication, the CH maintains the records of past interactions of another CH in the same manner as CMs keep interaction records of their neighbors.Thus, the direct trust value can be computed according to the number of successful and unsuccessful interactions. The BS periodically asks all CHs for their trust ratings on their neighbors. After obtaining the ratings from CHs, the BS will aggregate them to form an effective value of ITD.

Similar to the trust decision-making process at the CM level,in LDTS, the ITD of a CH only depends on the feedback reported by the BS. Thus, in the CH-to-CH communication case, when a CH wants to interact with another CH , it will send a feedback request to the BS, at the maximum. Therefore, including the response message form the BS, the total communication overhead is two packets. Thus, this mechanism can also greatly reduce network communication overhead and consequently improve the system's resource efficiency.

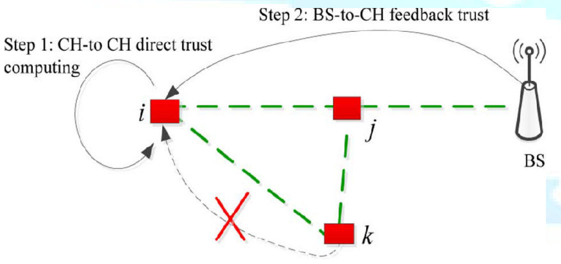
Step 2: BS-to-CH feedback trust
Step 1: CH-to CH direct trust computing
i
j
k
BS

Fig. 3. Trust decision-making at CH level.

C. Summary of Trust Relationships in LDTS

As shown in Figs. 2 and 3,LDTS needs to maintain two levels of trust: intercluster trust and intracluster trust. Intracluster trust evaluation has two kinds of trust relationship: *CM-to-CM* direct trust and *CH-to-CM* feedback trust. Likewise, intercluster trust evaluation also has two kinds of trust relationship, *CH-to-CH* direct trust and *BS-to-CH* feedback trust.

C. A secure trust system using RC4 algorithm

Compared with conventional desktop computers, severe challenges exist – sensors have limited processing, storage, bandwidth and energy. So light-weight is an important characteristic for the design of the secure protocol of sensor networks.RC4 is probably the most widely used stream cipher in the world due to its simplicity and efficiency[16],[17]. RC4 algorithm is a variable key-size stream cipher scheme based on a secret internal state of 256 bytes and two pointers. The data is encrypted by XORing data with the cipher stream generated by RC4 from an RC4 key. RC4 includes two parts: a Key-Scheduling Algorithm (KSA) which turns a random key into an initial permutation S, and a Pseudo-Random Generation Algorithm (PRGA) which uses this permutation to generate a pseudo-random output sequence to be the cipher stream.

Algorithm 2

RC4 Algorithm:

```
PRGA (S)
Initialization
i←0
j←0
Generation loop:
i←(i+1)mod256
j←(j+S[i])mod256
S[i]↔S[j]
Output z← +S[S[i]+S[j]mod256]
IPRGA(S,i,j)
Generation loop:
S[i]↔S[j]
j←(j-S[i]+256)mod256
i←(i-1+256)mod256
Output z←S[(S[i] + S[j])mod256]
```

Before the transmission, the sender and receiver share the RC4 base key, the offset value, the number of packets n, and the fixed-length value F through sender-to-receiver authenticated channel. Firstly, both sides (the sender and receiver) process the RC4-KSA and get the initialization state of S. Secondly, after applying offset rounds of RC4-PRGA, both sides apply RC4-PRGA for key stream generation as shown in Figure 4. Both sender and receiver reset their SC to zero.

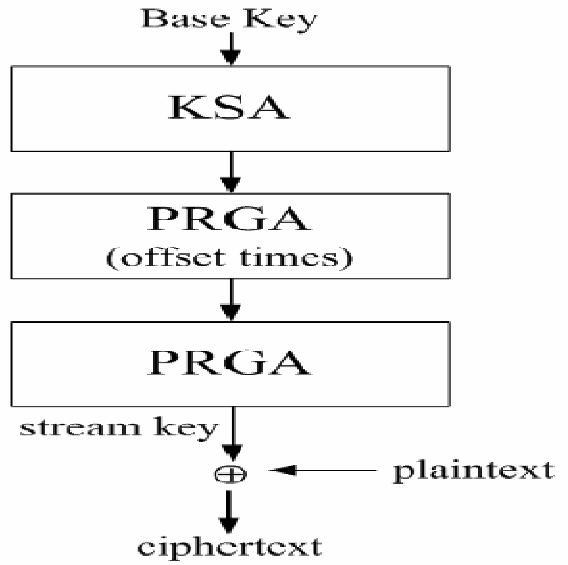

Figure 4: Flowchart of the improved RC4 algorithm

The sender divides the plaintext into one or several fixed-length data packet(s). If there are not enough data in the last fixed-length data packet, fill in random numbers in the rest of space. The sender begins to encrypt the fixed-length data packets. First, the sender increases the SC by one (SC=1) and encrypts the first packet plaintext by applying RC4-PRGA F rounds. In each round, a stream key (byte) is generated to XOR with the next data (byte) of the packet. The encrypted packet is then sent out. Apply the same steps to the rest of the data packets stream. When receiver gets a packet and compares the SC received with its own SC, it is easy to calculate out the suitable key stream to decrypt this packet by the reversible nature of RC4 state, and then XOR them with the encrypted data packet to restore the corresponding fixed-length data packet. The receiver can use this way to decrypt all received packets, and combine them into the entire input plaintext. By using offset, the proposed protocol makes effective use of RC4's strengths, and minimizes or eliminates most of its weaknesses. The proposed secure protocol can be used in most applications, not only one-to-one secure transmission, but also broadcasting and multicasting.

4. Conclusion

This model can greatly improve system efficiency while reducing the effect of malicious nodes. By adopting a dependability-enhanced trust evaluating approach for cooperation's between CHs, LDTS can effectively detect and prevent malicious, selfish, and faulty CHs. Due to canceling feedback between cluster members (CMs) or between cluster heads (CHs), this approach can significantly improve system efficiency while reducing the effect of malicious nodes. The proposed secure protocol can be used in most applications, not only one-to-one secure transmission, but also broadcasting and multicasting. Theory as well as simulation results show that this model demands less memory and communication overhead as compared with other typical trust systems and is more suitable for clustered WSNs.

References

[1] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensornetworks,"*IEEE Trans. Wireless commun.*, vol. 1, no. 4, pp. 660–670,Oct. 2002.

[2] D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," *Comput. Commun.*, vol. 32, no. 4, pp. 662–667, Apr. 2009.

[3] Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, "An energy-efficient clustering solution for wireless sensor networks," *IEEE Trans.WirelessCommun.*, vol. 10, no. 11, pp. 3973–3983, Nov. 2011.

[4] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc sensor networks," *IEEETrans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct. 2004.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. SensorNetw.*, vol. 4, no. 3, pp. 1–37, May 2008.

[6] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans.*

Depend.Secure Comput., vol. 9, no. 2, pp. 184–197, Apr. 2012.

[7] A.RezguiandM. Eltoweissy, " mRACER: A reliable adaptive service driven efficient routing protocol suite for sensor-actuator networks,"*IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 5, pp. 607–622, May 2009.

[8] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," *Wireless Netw.*, vol. 16, no. 5, pp.1493–1510, Jul. 2010.

[9] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. ACM Workshop Security ofad hoc and Sensor Networks (SASN'04)*, Oct. 2004, pp. 66–67.

[10] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," in *Proc. ThirdIEEE Int. Conf. Mobile Ad-Hoc and Sensor Systems (MASS'06)*, Oct. 2006, pp. 437–446.

[11] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in *Proc. SecondIEEEWorkshop on Dependability and Security in Sensor Networks andSystems*, 2006, pp. 10–22.

[12] A. Boukerche, X. Li, and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Commun.*, vol. 30, pp. 2413–2427, Sep. 2007.

[13] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

[14] L. Qing, Q. Zhu, and M. Wang, "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks," *ComputerCommun.*, vol. 29, pp. 2230–2237, 2006.

[15] A. Bari, A. Jaekel, and S. Bandyopadhyay, "Clustering strategies for improving the lifetime of two-tiered sensor networks," *Computer Commun.*, vol. 31, pp. 3451–3459, 2008

.

[16] A. Perrig, R. Szewczyk, V. Wen, D.Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *Wireless Networks*, 2002, pp 521-534

[17] S. Michell, K. Srinivasan, "State Based Key Hop Protocol: A Lightweight Security Protocol for Wireless Networks", *1st ACM International Workshop onPerformance Evaluation of Wireless Ad Hoc, Sensor, andUbiquitous Networks*, Venice, Italy. October 4, 2004, pp 112-118.