A Secure EDTM For Wireless Sensor Network

Nefilda K Joseph
dept. electronics and communication
Nehru college of engineering and research centre
Thrissur, India
nefildakjoseph@gmail.com

Jithin Jose Kallada
dept. electronics and communication
Nehru college of engineering and research centre
Thrissur, India
jithinjosekallada@gmail.com

***Abstract*— Trust is an important factor in transferring data from the source to destination in wireless sensor networks. If any sensor node fails to transfer the data Protocol calculates the alternate path. Trust models have been recently suggested as an effective security mechanism for Wireless Sensor Networks (WSNs). Considerable research has been done on modeling trust. However, most current research work only takes communication behavior into account to calculate sensor nodes' trust value, which is not enough for trust evaluation due to the widespread malicious attacks. In this paper propose a Secure Efficient Distributed Trust Model (EDTM) for WSNs. First, according to the number of packets received by sensor nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust. Furthermore, trust reliability and familiarity are defined to improve the accuracy of recommendation trust. In this proposed the method using a modification of cryptographic algorithm. In which find an alternate path in presence of a deactivated node in the rout.**

Keywords—EDTM,WSNs,Trust,cryptographic algorithm

I. INTRODUCTION

WSNS are emerging technologies that have been widely used in many applications such as emergency response [1], healthcare monitoring [2], battlefield surveillance, habitat monitoring, traffic management, smart power grid [3], etc. However, the wireless and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Thus, providing security is extremely important for the safe application of WSNs. Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. However, these approaches still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes. To establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish a trust model allowing a sensor node to infer the trustworthiness of another node.
Nowadays, many researchers have developed trust models to build up trust relationships among sensor nodes [4].
For example in [5], a distributed Reputation-based Framework for Sensor Networks (RFSN) is first proposed for WSNs. Two key building blocks of RFSN are Watchdog and Reputation System. Watchdog is responsible for monitoring communication behaviors of neighbor nodes. Reputation System is responsible for maintaining the reputation of a sensor node. The trust value is calculated based on the reputation value. However, in RFSN, only the direct trust is calculated while the recommendation trust is ignored. A Parameterized and Localized trust management Scheme (PLUS) is proposed in[3]. In PLUS, both personal reference and recommendation are used to build reasonable trust relationship among sensor nodes. Whenever a judge node (the node which performs trust evaluation) receives a packet from suspect node (the node which is in radio range of the judge node and will be evaluated), it always check the integrity of the packet. If the integrity check fails, the trust value of suspect node will be decreased irrespective of whether it was really involved in malicious behaviors or not. Therefore, suspect node may get unfair penalty. Another similar trust evaluation algorithm named as Node Behavioral strategies Banding belief theory of the Trust Evaluation algorithm (NBBTE) is proposed based on behavior strategy banding D-S belief theory. NBBTE algorithm first establishes various trust factors depending on the communication behaviors between two neighbor nodes.

Then, it applies the fuzzy set theory to measure the direct trust values of sensor nodes. Finally, considering the recommendation of neighbor nodes, D-S evidence theory method is adopted to obtain integrated trust value instead of simple weighted-average one. To the best of our knowledge, NBBTE is the first proposed algorithm which establishes various trust factors depending on the communication behaviors to evaluate the trustworthiness of sensor nodes. Therefore, NBBTE is chosen as the comparing algorithm in this paper.

From the literature on this topic, we can find that: 1) In the current research work, the assessment of trust values for sensor nodes is mainly based on the communication (successful and unsuccessful communications) point of view. In fact, just considering the communication behavior, we cannot decide whether a sensor node can be trusted or not. Besides the communication behavior, other trust metrics such as the energy level should also be taken into account to calculate the trustworthiness of sensor nodes. In addition, an efficient trust model should deal with uncertainty caused by noisy communication channels and unstable sensor nodes behaviors. 2) There are two common ways to establish trust in WSNs: calculating direct trust based on direct interactions and calculating indirect trust value based on recommendation from the third party. However, not all the third parties are trusty and not all the recommendations are reliable. Thus, a discriminate analysis about the third party and recommendation is essential. 3) Most existing studies only provide the trust assessment for neighbor nodes. However, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbor nodes. For example, in some routing protocols (e.g., TPGFPlus [8]) or localization algorithms (e.g., improved LMAT algorithm [9]), sensor nodes need the information of the two-hop neighbor nodes to establish the routing or localize themselves. Therefore, providing the trust assessment for non-neighbor nodes becomes very important. 4) Because of the dynamic topology, the trust relationship between sensor nodes constantly changes in WSNs.

Trust is a dynamic phenomenon and changes with time and environment conditions. However, most existing trust models do not solve the trust dynamic problem. The evolution of trust over time is another problem that needs further study. In order to solve the above-mentioned problems, we propose an efficient distributed trust model (EDTM).

The proposed EDTM can evaluate the trust relationships between sensor nodes more precisely and can prevent security breaches more effectively. The rest of the paper is organized as follows: In Section II, the assumptions and network model are introduced. In the Section, the overview of EDTM is presented. Finally, the performance of the EDTM is evaluated.

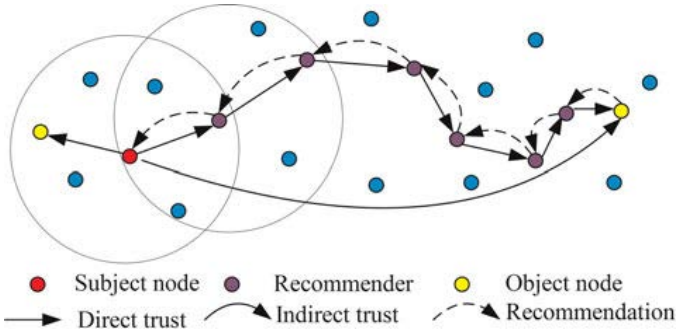

Fig. 1:The Network Structure

II. Assumptions and Network Model

In this paper, we consider a scenario in which all the sensor nodes are randomly deployed without mobility. As shown in Fig. 1, there are three kinds of nodes in the network: subject nodes, recommender and object nodes. If a sensor node A wants to obtain the trust value of another sensor node B, the evaluating sensor node A is named as subject node and the evaluated node B is the object node. This paper is a multi-hop network which means that the sensor nodes can only directly communication with the neighbor nodes within their communication range. The packets exchanged between any two non neighbor nodes are forwarded by other nodes. The forwarding node not only can just “pass” the packets from source nodes to destination nodes but also can process the information based on their own judgments. Generally, the trust value is calculated based on a subject’s observation on the object and recommendations from a third party. The third party which provides recommendations is a recommender. Node capability. It assumes that sensor nodes have the same capability of computing, communicating and storing. Their communication ability is limited by specific wireless techniques. Only when two nodes move into each other’s communication range could they detect each other and start communication. A homogeneous WSN is considered, that is all the sensor nodes have the same initial energy level and communication range. Additionally, in order to secure data transmission over the wireless network, each node is assigned a unique ID and a pair of public/private keys for encrypting and decrypting data, as well as with a public key certificate issued by some trustable Public Key Infrastructure (PKI). Each node keeps a list of neighbor nodes which stores their IDs and their communication information.

Attack model. There exist many malicious attacks in WSNs, such as DoS attack, node replication, Sybil attack, wormhole attack, attacks on Information, etc. Moreover, it should be noticed that similar to most security schemes, a trust model is also vulnerable to many malicious attacks, such as bad/good-mouthing attack and on-off attack. In a bad-mouthing attack, malicious nodes intentionally give dishonest recommendation to neighbor nodes. For example, they maliciously provide lower recommendation for normal ones during trust evaluation. Thus, recommendations under bad-mouthing attack cannot reflect the real opinions of the recommender. On the contrary, the sensor nodes conducting good-mouthing attack intentionally provide higher trust value for malicious nodes. In an on-off attack, malicious nodes can behave good or bad alternatively. When the trust values of malicious nodes are significantly reduced, they can act well for a period to improve their trust values. Therefore, it is difficult to detect these malicious nodes by conventional trust models.

III. OVERVIEW OF EDTM

To efficiently compute the trust values on sensor nodes, we first need a clear understanding of the trust definition and the various trust properties that are adopted in a trust model.

A. Definition And Properties Of Trust

There are several definitions given to trust in the literature [10]. Trust is always defined by reliability, utility, availability, risk, quality of services and other concepts.

Here, trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviors. That is, the trust value is used to reflect whether a sensor node is willing and able to act normally in WSNs.

In this paper, a trust value ranges from 0 to 1. A value of 1 means completely trustworthy and 0 means the opposite. Direct trust is a kind of trust calculated based on the direct communication behaviors. It reflects the trust relationship between two neighbor nodes.

As mentioned above, since the recommendations from third parties are not always reliable, we need an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust. When a subject node cannot directly observe an object nodes communication behaviors, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes. Based on [1] and [2], we can conclude that there are three main properties of trust: asymmetry, transitivity and composability. Asymmetry implies that if node A trusts node B, it does not necessarily mean that node B trusts node A. Transitivity means the trust value can be passed along a path of trusted nodes. If node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a certain level. The transitivity is a very important property in trust calculation between two non-neighbor nodes. Composability implies that trust values received from multiple available paths can be composed together to obtain an integrated value.

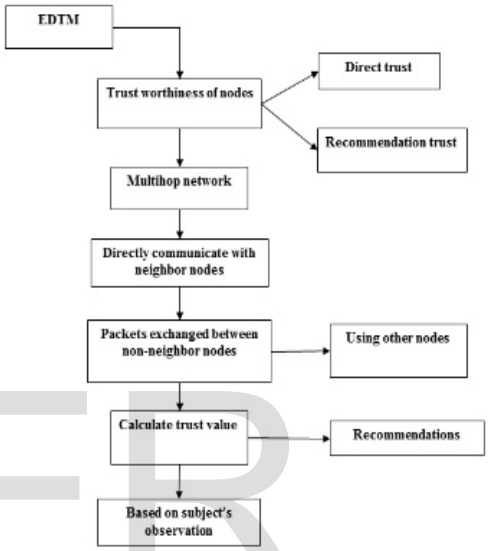

Fig. 2: The EDTM Structure

B. The Structure Of EDTM

In this section, we describe the overall architecture of EDTM. When we say node B is trustworthy or untrustworthy for node A, there is a trust model between node A and node B. As shown in Fig. 2, EDTM consists of two main components: one-hop trust model and multi-hop trust model which includes the following six components: direct trust module, recommendation trust module, indirect trust module, integrated trust module, trust propagation module and trust update module. When a subject node wants to obtain the trust value of an object, it first checks its recorded list of neighbor nodes. If the ID of the object node is in the list of neighbor nodes, the one-hop trust model is triggered. Otherwise, the multi-hop trust model is started. In the one hop trust model, if the trust is calculated based on node B's direct experiences with node A completely, this model is called

direct trust model. Otherwise, the recommendation trust module is built. In the multi-hop trust model, once the subject node A receives recommendations from other nodes about the object node B, indirect trust model can be established.

In current trust models, the direct trust and recommendation are always used to evaluate the trustworthiness of sensor nodes. The direct trust is directly calculated based on the communication behaviors between two neighbor nodes. However, due to malicious attacks, using only direct trust to evaluate sensor nodes is not accurate. Thus, the recommendation from other sensor nodes is needed to improve the trust evaluation. In addition, if the number of communication packets between two neighbor nodes is too small, it is difficult to decide whether an object node is good or bad based on only few interactions. Therefore, in the one-hop trust model, we define a threshold of communication packets Th_{num}. If the communication packets between the subject and object nodes are higher than the threshold Th_{num}, only the direct trust is calculated. Otherwise, the recommendations from the recommenders are needed for the object's trust evaluation.

In the multi-hop trust model, the subject node first needs to select a set of recommenders. Then, the indirect trust is calculated based on recommendations and trust propagation. Next, we describe the detail calculation of direct, recommendation, and indirect trust.

C. The Calculation Of Direct Trust

We compose our direct trust by considering communication trust, energy trust and data trust. The sensor nodes in WSNs usually collaborate and communicate with neighbor nodes to perform their tasks. Therefore, the communication behaviors are always checked to evaluate whether the sensor node is normal or not. However, due to the nature of wireless communication, there are many reasons resulting in the packets loss and the communications between sensor nodes are unstable. The unsuccessful communication maybe caused by malicious nodes or unstable communication channel. Therefore, just evaluating the communication behaviors is not enough for trust evaluation. In addition, it is generally known that all communications in WSNs will consume a certain amount of energy to transmit some data packets or any information. If there are malicious nodes in WSNs, the abnormal energy will be consumed or the transmitted data packets will be falsified to conduct malicious attacks. Therefore, communication trust, energy trust and data trust are defined in EDTM. The communication trust reflects if a sensor node can cooperatively execute the intended protocol. The energy trust is used to measure if a sensor node is competent in performing its intended functions or not. The data trust is the trust assessment of the fault tolerance and consistency of data, which affects the trust of the sensor nodes that create and manipulate the data.

D. Calculation of the Communication Trust

The information on a sensor node's prior behavior is one of the most important aspects of the communication trust. However, communication channels between two sensor nodes are unstable and noisy, thus monitoring sensor node's behaviors in WSNs based on previous communication behaviors involves considerable uncertainty. To deal with this uncertainty, we adopt a Subjective Logic framework [3]. The trust value in SL framework is a triplet $T \in \{b, d, u\}$ where b, d and u correspond to belief, disbelief and uncertainty respectively, $b, d, u \in [0,1]$, $b + d + u = 1$. Following the trust model based on Subjective Logic framework [14], the communication trust Tcom is calculated based on successful (s) and unsuccessful (f) communication packets.

$$Tcom = (2b+u)/2$$

where $b = s/(s+f+1)$, $u = 1/(s+f+1)$

E. Calculation of the Energy Trust

Energy is an important metric in WSNs since sensor nodes are extremely dependent on the amount of energy they have. Malicious nodes always consume abnormal energy to launch malicious attacks. For example, malicious nodes which conduct DoS attack consume much more energy than normal nodes while selfish nodes consume less energy. Therefore, we use energy as a QoS trust metric to measure if a sensor node is selfish or maliciously exhaust additional energy. Using an energy prediction model, sensor nodes energy consumption in can different periods can be obtained. If the environment conditions do not change much, the energy consumption rate of normal nodes maintain a stable value.

F. Calculation of the Data Trust

Following the idea introduced in [2]: the trust of the data affects the trust of the network nodes that created and manipulated the data, and vice-versa, we introduce the

evaluation of data trust in this section. The data packets have spatial correlation, that is, the packets sent among neighbor nodes are always similar in the same area. The data value of these packets in general follows some certain distribution, such as a normal distribution. For the sake of simplicity, in this paper, we also model the distribution of the data as a normal distribution.

G. Calculation of Recommendation Trust

The recommendation trust is a special type of direct trust. When there are no direct communication behaviors between subject and object nodes, the recommendations from recommender are always taken into account for trust calculation. However, in most existing related works, the true and false recommendations are not distinguished. How to detect and get rid of false recommendations is important since it has great impact on the trust calculation.

As shown in Fig. 3, when a subject node A wants to obtain the recommendations of an object node B. The subject node A first checks its trust records and then selects a set of common neighbor nodes of node A and node B as the recommenders C1;C2; . . . ;Cn, which have the trust value larger than the threshold 0.5. Subsequently, subject node A transmits a recommendation request message to the selected recommenders through multi-casting. Obviously, the identity of node B should be added into the recommendation request. Upon receiving a request message, the qualified nodes will reply if they have recommendation of node B. Based on the recommendations, the subject node A filters the false recommendation and compute the recommendation trust of node B.

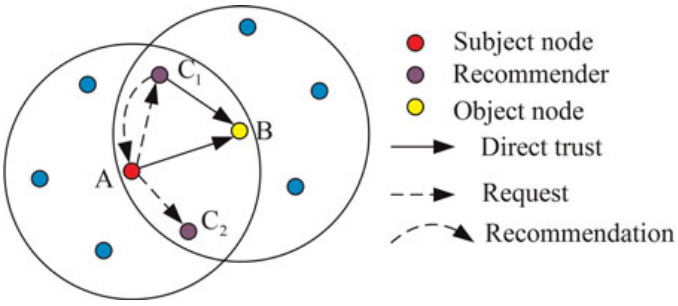

Fig. 3 :Calculation Of The Recommendation Trust

H. Calculation of the Indirect Trust

WSNs are multi-hop networks, when there are no direct communications between subject and object nodes, indirect trust can be established since trust is transitive. In this paper, the calculation of indirect trust includes two steps:

The first step is to find multi-hop recommenders between subject and object nodes, and the second step is the trust propagation which aims at computing the direct trust. The path from the subject node to the object node established by the recommenders is named as Trust Chain. As shown in Fig. 4, based on the location information of sensor nodes, we observe three different kinds of mechanisms for choosing the recommender in this paper:

Finding a recommender which is closest to the object node to save energy consumption, finding a recommender which has the highest trust value to guarantee the reliability of Trust Chain and finding an optimal Trust Chain by both considering the distance information and the trust value. The first selection mechanism can find the shortest Trust Chain, thus the communication overhead for indirect trust calculation can be minimized.

However, in this case, the indirect trust evaluation is not accurate because malicious nodes maybe chosen as recommenders. While the second selection mechanism can choose the most believable Trust Chain but this Trust chain is not energy efficient. Relatively speaking, the third selection mechanism is the best one.

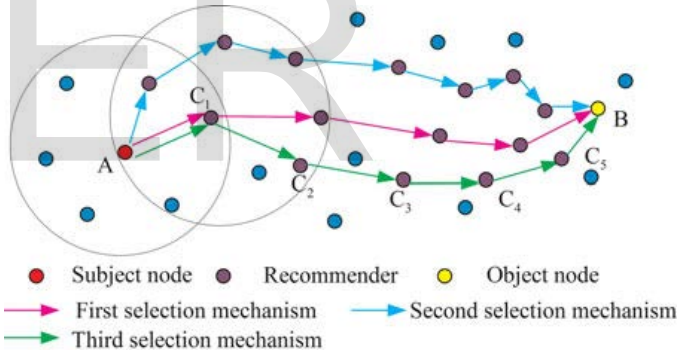

Fig. 4: Calculation Of The Indirect Trust

IV. PERFOMANCE OF EDTM

The trust model has become important for malicious nodes detection in WSNs. It can assist in many applications such as secure routing, secure data aggregation, and trusted key exchange. Due to the wireless features of WSNs, it needs a distributed trust model without any central node, where neighbor nodes can monitor each other. In addition, an efficient trust model is required to handle trust related information in a secure and reliable way. If any node inactive in between source and destination then the probability of

attacking the node increases. Hence, the proposed model with using an modified algorithm in key generation. In which, find an alternate path in presence of the deactivated node.

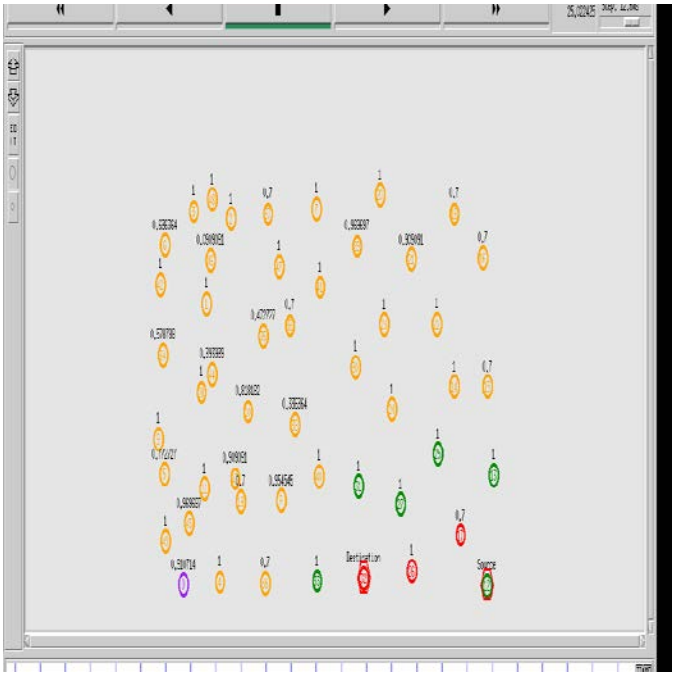

Fig. 5: Simulated output of EDTM

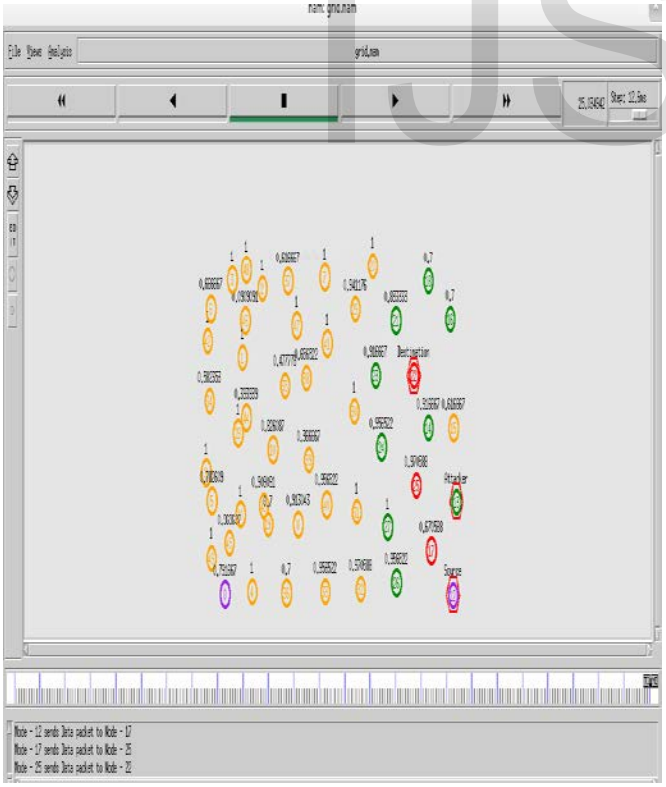

Fig. 6:Simulated output of EDTM in presence of the attacker

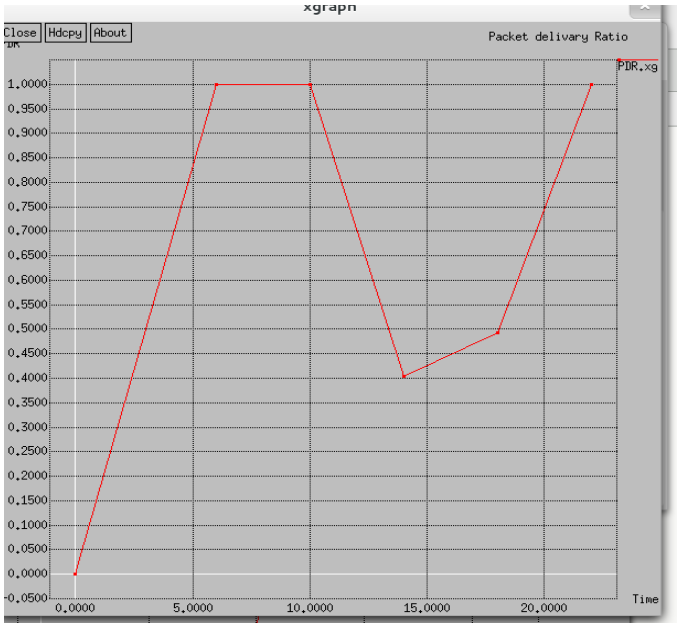

Fig. 7: Packet delivery ratio

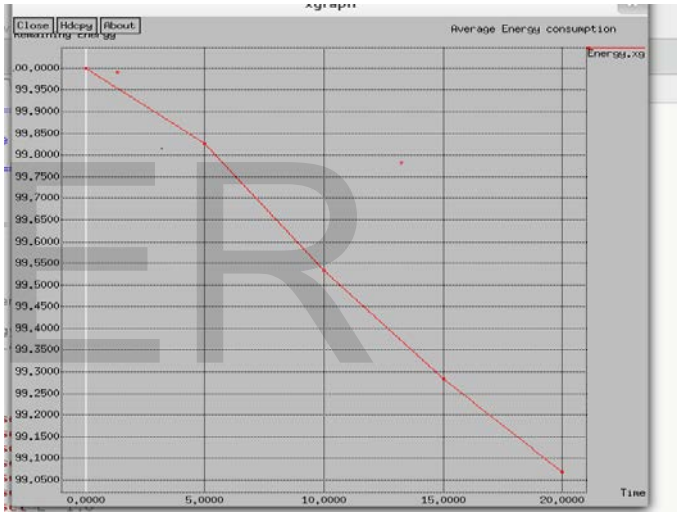

Fig. 8: Average energy consumption

References

[1] G. Han, Y. Dong, H. Guo, L. Shu, and D. Wu, "Cross-layer optimized routing in WSN with duty-cycle and energy harvesting,"Wireless Commun. Mobile Comput., 3 Feb. 2014, DOI: 10.1002/wcm.2468.

[2] G. Han, X. Xu, J. Jiang, L. Shu, and N. Chilamkurti, "The insights of localization through mobile anchor nodes in wireless sensor networks with irregular radio," KSII Trans. Internet Inf. Syst., vol. 6, pp. 2992–3007, 2012.

[3] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile ad hoc networks: A survey," IEEE Commun Surveys Tuts.,

vol. 14, no. 2, pp. 279–298, 2nd Quarter 2012.
[4] A. Josang, "An algebra for assessing trust in certification chains," in Proc. Netw. Distrib. Syst. Security Symp., 1999, pp. 1–10.
[5] W. Gao, G. Zhang, W. Chen, and Y. Li, "A trust model based on subjective logic," in Proc. 4th Int. Conf. Internet Comput. Sci. Eng.,2009, pp. 272–276. vol. 1, p. 13, 2007.
[6] H. S. Lim, Y. S. Moon, and E. Bertino, "Provenance based trustworthiness assessment in sensor networks," in Proc. 7th Int. Workshop Data Manage. Sens.