INTERNATIONAL JOURNAL OF COMPUTATIONAL MATHEMATICAL IDEAS ISSN: 0974-8652

Optimization For WSN's Using Advanced Reducing Energy Cost Based Trust System

Mr. Kavuri Lakshmi Ranganadha Simha [1] D Rammohan Reddy [2]

Newtons Institute of Engineering

Published in Volume 10, Issue 1 July-Aug: 2016, Page No: 65033 to 65042

Abstract—Watchdog technique is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). Unfortunately, this kind of technique consumes much energy and hence largely limits the lifespan of WSN. Although the state-of-the-art studies have realized the importance of trust systems' efficiency in WSNs and proposed several preliminary solutions, they have overlooked to optimize the watchdog technique, which is perhaps among the top energy-consuming units. In this paper, we reveal the inefficient use of watchdog technique in existing trust systems, and thereby propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the system's security in a sufficient level. We have evaluated our algorithms through experiments on top of a WSNET simulation platform and an in-door WSN testbed in our collaborative lab. The results have successfully confirmed that our watchdog optimization techniques can save at least 39.44% energy without sacrificing much security (<0.06 in terms of trust accuracy and robustness), even in some cases enhance the protection against certain attacks.

Key Terms-

1. Wireless sensor network security
2. Trust system
3. Energy-efficiency
4. Watchdog technique.

I. INTRODUCTION

AS A CRITICAL complement to traditional security mechanisms (e.g., cryptographic methods [1], authentication [2] and access control logics [3] etc.), trust systems are widely applied to protect wireless sensor networks (WSNs for short) from being attacked by "legitimate" sensor nodes (i.e., the nodes are either compromised or selfish or on ault) [4]–[12]. Those nodes can bypass traditional security protections using their "legitimate" identities, but can be possibly captured by trust systems due to their poor reputation or past misbehavior [13]. That is, trust is built upon sensor nodes' reputation and past behaviors, and can be used to model these nodes' honesty and internal states. Although many trust systems [14] enable trust recommendations to extend the trust from neighborhood (i.e., direct trust) to a global network view (i.e., indirect trust), the direct experience of past behaviors is still the basis for securing those recommendations. In another word, sensor nodes' past behaviors constitute the basic foundation for building WSN's trust systems (WSNTSs for short).

However, collecting enough past behaviors through business traffic to build a reliable trust system for WSN is not a trivial task. First, the powerful base station (when WSN has a flat topology [15]) and cluster heads (when a hierarchical topology [16]), both of which are likely to have business requirements to interact with the whole network (or the entire cluster), may not locate in the communication range (i.e., neighborhood) of all sensor nodes (i.e., some nodes are remote), hence missing the opportunity to have direct experiences of those remote nodes. Second, some sensor nodes may not have business requirements to interact with their neighbour nodes, or their business interactions occur at a very low frequency. Those lazy nodes' past behaviors are hard to be collected using business traffic. Third, since trust is context aware [17], [18], the experience of one kind of behaviors cannot be used to build up trust for another kind. For example, a node behaving well to forward routing packets in the past does not mean the sensing data reported from this node is trustworthy (i.e., past multi-hop routing behaviors cannot derive the trust for data sensing). As a result, WSN may lack a wide variety of business traffic to build up all kinds of trust. To tackle those challenges and facilitate past behavior collection, most of existing WSNTSs have adopted a so-called watchdog technique [19]. Using this technique, sensor nodes can operate as proactive monitors and launch trust-dedicated tasks in a pre-defined frequency to directly interact with their neighborhood nodes. They thus can get the first-hand experiences of these nodes' behaviors, even if no business tasks happen. For example, a node can actively query other nodes' sensing data in some time interval [6] (despite it does not actually require those data for business purpose), or continuously overhear its neighborhood's routing communications through the promiscuous mode [4], [20].Although the watchdog technique has been proved as a very effective approach to build up WSNTS's foundations, it introduces a large amount of additional energy consumptions which conflict the energy efficient design principle of WSN. More precisely, sensor nodes are usually equipped with limited battery, and work in an unattended mode for a long period of time to adapt various harsh environments such as the deep desert and ocean abyss. Rechargement or replacement of those nodes' power is very difficult and expensive. Due to those challenges, energy saving plays a very important role in the design of modern WSNs [21]. However, to our best knowledge, no existing WSNTSs give appropriate solutions to save the energy consumed by the watchdog technique (i.e., the

Trust-energy conflict induced by watchdog usage has not been addressed before). In particular, some WSNTSs do not discuss how to schedule watchdogs in their proposals [20], [22], while some others implicitly suggest to let sensor nodes launch neighbour-flooding watchdog tasks to monitor all their neighbors and do not study which frequency is appropriate for their monitoring [4], [6], [23]. This kind of neighbour-flooding methods could make running watchdogs redundant and will waste a lot of energy without inducing much additional security benefits. As a result, to simultaneously save energy and collect sufficient past behaviors for trust evaluation, an intelligent watchdog scheduler is highly required In this paper, we will fill in this gap by optimizing watchdog techniques for WSNTSs to balance energy efficiency and security (in terms of trust accuracy and robustness). Our ultimate goal is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level. To touch this goal, we

optimize watchdog techniques in two levels. First, we optimize watchdog locations by considering the fact: although sensor nodes which are located more closely may consume less energy to monitor each other due to shorter communication distance [24], these nodes are more likely of being compromised together and launch collaborative attacks [25].

We therefore explore the optimal watchdog location (given a target node) to minimize the overall risk (in terms of both energy consumption and security). Second, we optimize watchdog frequency and reduce its redundancy. In particular, compared with the sensor nodes whose behaviors are more uncertain, the nodes with more determined trustworthiness (i.e., trustworthy or untrustworthy) may require less watchdog tasks (i.e., lower watchdog frequency) to further investigate. We thus seek appropriate watchdog frequency depending on target nodes' trustworthiness.

To sum up, we make three major contributions in this paper.

1) We conduct a novel study to reveal trust-energy conflict induced by the inefficient use of watchdog techniques in
existing WSNTSs. This conflict has not been comprehensively addressed by prior research in the literature.

2) We optimize watchdog techniques in two levels, both of which consist of a theoretical analysis to show potential
optimal results and a practical algorithm to efficiently and effectively schedule watchdog tasks.

3) We evaluate our optimization techniques using extensive experiments in a WSNET simulation
platform [26] and an in-door testbed in our collaborative lab. The experimental results have successfully
confirmed the effectiveness of our design.

The remainder of this paper is structured as follows.

We first review the literature in Section II. We then give a high level overview of WSN and WSNTS models
in Section III. We present our watchdog optimization algorithms in Section IV, and evaluate these algorithms
in Section V. After discussing some limitations and potential future works in Section VI, we conclude this paper
in Section VII.

Methodology

MODEL OVERVIEW

In this section, we formalize WSN and WSNTS using four high level models. More precisely, we first present a
system model to describe WSN in Section III-A. We then model WSN's energy consumption law in Section III-B.
Afterwards, we reason about WSNTS on top of a threat model in Section III-C and a trust model in Section III-D, respectively.

For the ease of reference, we summarize important notations used by this paper in Table I.

A. System Model

We model a WSN as an undirected graph G = (V, E), where vi ∈ V represents a sensor node in WSN and ei j ∈ E
means that the nodes vi and v j are within each other's communication range (i.e., neighborhood). We design our
methods by considering a flat WSN topology, although our solutions work within the scope of neighborhood and thus also adapt to other topologies such as the clustering WSN. Let di j be the spatial distance between vi and v j, and let ri be the communication range of vi . We consider that ei j ∈ E exists

TABLE I
IMPORTANT NOTATIONS

Notation	Definition
$G = (V, E)$	An undirected graph used to model a WSN
v_i	$v_i \in V$ represents a sensor node in WSN
r_i	v_i's communication range
d_{ij}	The spatial distance between v_i and v_j
e_{ij}	$e_{ij} \in E$ exists iff $d_{ij} \leq r_i$ & $d_{ij} \leq r_j$
B_j	The set of v_j's neighborhood nodes
W_j	The set of v_j's watchdog nodes
ϵ	The free space constant measured in J/bit/m^2
t	A discrete time slot, the minimal time unit in this paper
N	A time window consists of a sequence of discrete time slots
w_{ij}^t	The watchdog task v_i performs to monitor v_j at time slot t
L	The bits of information transmitted by a watchdog task
A	The set of sensor nodes under attackers' control in WSN
α	A parameter to control the probability of collaborative attackers
T_{ij}	v_j's trustworthiness from v_i's point of view
Λ_{ij}	The accuracy of T_{ij} (trust accuracy)
Υ_j	The average accuracy of T_{ij}s for $\forall v_i \in W_j$ (trust robustness)
I_{ij}^t	The event representing whether v_j's behavior is expected by v_i at t
$\mathbf{Q}_{ij}$	The distribution of I_{ij}^ts for $t \in N$
I_j^t	the event to represent v_j's true internal behavior at t
$\mathbf{P}_j$	The distribution of I_j^ts for $t \in N$
f_{ij}	Watchdog frequency v_i uses to monitor v_j
f_j	A sensor node v_j's internal behavior frequency
fa_j	A sensor node v_j's attacking/faulty behavior frequency
fn_j	A sensor node v_j's normal behavior frequency
π_i	Used by DBP algorithm to determine the size of W_i
μ	Used by HWFA(E) algorithm to keep watchdog redundancy

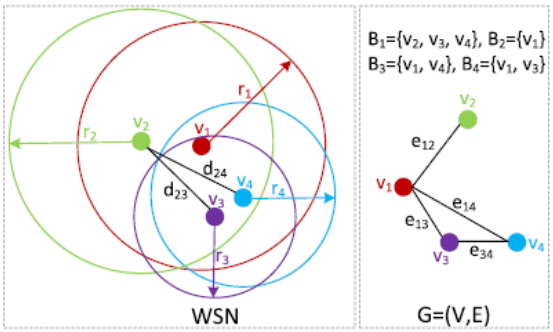

Fig. 1. An example of WSN and the system model G.

iff di j ≤ ri and di j ≤ r j . We therefore define Bi ⊆ V as the set of vi 's neighborhood nodes. We have Bi = {v j |ei j ∈ E} ={v j |di j ≤ ri & di j ≤ r j }. Figure 1 gives an example of our WSN system model. As can be seen, although v3 and v4 are within v2's communication range (i.e., d23 ≤ r2 and d24 ≤ r2),
e23 and e24 do not exist (i.e., v3, v4 /∈B2) because d23 > r3 and d24 > r4.

To formalize a watchdog task on top of G, we first separate time space into a sequence of consecutive time slots with equal size. We then define wti j as a watchdog task the node vi performs to monitor its neighbor node v j at time slot t.A watchdog task wti j consists of a bidirectional communication between the watchdog node vi and the target node v j. That is, vi should send a request packet to v j and then wait for v j 's response. By this requirement, vi can take watchdog task wt i j to monitor v j iff di j ≤ ri and di j ≤ r j (i.e., ei j exists in G). In another word, the node vi can work as a watchdog to monitor only ∀v j ∈ Bi , and vice versa, only ∀v j ∈ Bi can perform watchdog tasks to monitor vi .

B. Energy Consumption Model

To estimate energy consumed by each watchdog task wt i j , we follow a typical free space wireless radio model, which is widely adopted by the literature (e.g., LEACH [24]). In this model, a sensor node's transmitter unit consists of a transmit electronics device and a power amplifier, both of which will consume energy when transmitting signals. In contrast, a node's receiver unit only consumes energy due to the receive electronics device. We follow prior research like [24] and [29] to assume that a proper power controller has been deployed to adjust transmit power amplifier according to the transmission distance. Let elect be the energy consumed by a sensor node's transmit electronics (or receive electronics) when sending (or receiving) 1 bit information (measured in J/bit). Let _ be free space constant measured in J/bit/m2. We then can calculate the energy consumption when vi transmits 1 bit information to its neighbor node v j (di j ≤ ri) as:

$$\varepsilon_{ij}^{TX} = \varepsilon^{elec} + \epsilon \cdot d_{ij}^2. \quad (1)$$

Meanwhile, the energy consumed by vi for receiving 1 bit information from neighbor node v j can be computed as:

$$\varepsilon_{ij}^{RX} = \varepsilon^{elec}. \quad (2)$$

As described in Section III-A, to accomplish a watchdog task wt i j , the watchdog node vi should first send query to
target node then receive target node's reply, while the target node v j should first receive the query from the watchdog node then send back the reply. As a result, if a watchdog task wt i j requires L bits information for either query or response, the energy consumed by the watchdog node vi for this task is:

$$\varepsilon_i(w_{ij}^t) = L \cdot (\varepsilon_{ij}^{TX} + \varepsilon_{ij}^{RX}) = 2 \cdot L \cdot \varepsilon^{elec} +$$

The target node v j 's energy consumption for this watchdog
task wti j is (note that di j = d j i):

$$\varepsilon_j(w_{ij}^t) = L \cdot (\varepsilon_{ji}^{RX} + \varepsilon_{ji}^{TX}) = 2 \cdot L \cdot \varepsilon^{elec} +$$

C. Threat Model

In our design, we assume some sensor nodes could be compromised or selfish or on fault. By exploiting those
"legitimate" nodes, we consider two kinds of attacking behaviors. One is for disrupting WSN's normal functionalities such as routing and data sensing, and the other is for attacking WSNTS itself. In particular, we consider the attacking capabilities as follows:
1) Attacking From "Legitimate" Sensor Nodes: We consider the attackers who are capable of compromising
some vulnerable sensor nodes or deploying malicious or faulty nodes to WSN. Attackers can exploit these nodes'
"legitimate" identities to break traditional security protections, and hence can launch offensives to the remainder of WSN.
Further, we consider the attacking model cooperative, where the nodes that are closer to an attacker's node are more likely of being controlled by the attacker as well [25]. We let A ⊆ V be the set of the "legitimate" sensor nodes under attackers' control. Then, given an attacker's node v j , the probability that another node vi is also under attacker's control is inversely proportional to di j :

$$Pr[v_i \in A | v_j \in A] \propto \frac{1}{\alpha \cdot d_{ij}}. \quad (5)$$

However, 1α·di j cannot be used as a probability function directly, because 1 α·di j belongs to [0,+∞] but a possible probability function should be falling into [0, 1]. To tackle this issue, we need to give a feasible probability definition that satisfies Pr[vi ∈ A|v j ∈ A] ∈ [0, 1] and Pr[vi ∈ A|v j ∈ A] ∝1α·di j simultaneously. To meet this requirement, we define the probability function as Pr[vi ∈ A|v j ∈ A] = 1α·di j+1 in this paper. This probability function is feasible and meaningful. In particular, WSN attackers usually exploit wireless signal to intrude sensor nodes. A longer distance leads to a weaker attacking signal, which represents a weaker attacking capability [25]. As a result, Eq. (5) can naturally reflect such wireless attacking scenario. More precisely, di j = 0 can lead Pr[v j ∈ A|vi ∈ A] = 1 since it indicates that vi and v j are the same node or different nodes located at the same position. While, with di j increasing, Pr[v j ∈ A|vi ∈ A] will decrease due to the weakening signal and can eventually reach 0 when di j approximates+∞. A larger α indicates a higher decreasing speed of Pr[vi ∈ A|v j ∈ A] when di j increases.
2) Attacking WSN: By exploiting the "legitimate" sensor nodes, attackers could perform insider attacks to disrupt
WSN's normal functionalities, such as damaging the quality of multihop routing by selectively dropping routing packets or misleading WSN's data aggregation by reporting crafted sensing data. Those attacks can avoid traditional security mechanism.

3) Attacking WSNTS: Moreover, we consider attackers smart enough and are aware of the existence ofWSNTS. Those attackers attempt to evade WSNTS's detection by launching some advanced attacks. In particular, we consider four types of WSNTS attacks in this paper (all of them have been widely considered in the literature [14], [18]). The first is an on-off attack, where attacker's node may behave well for a long time to get enough reputation then do malicious behaviors suddenly. The second is a discrimination attack where attacker's node will behave differently to different sensor nodes (watchdogs). The third is a bad-mouthing attack, where attacker's node
will perform watchdog tasks and report an honest node as a malicious one. The last is a sybil attack where attackers can control a large number of sensor nodes to mislead WSNTS.

D. Trust Model

In this paper, we model the trust of a sensor node as this node's expected behavior distribution over time. The behavior could be data sensing or routing behavior etc. This trust model can allow our analysis to be focused on WSNTS's foundation, and will not be affected by higher level's trust update and aggregation processes. On top of this model, we introduce three concepts. One is trustworthiness that can be used to estimate a sensor node's behavior. The other two are trust accuracy and trust robustness, which can be used to measure how accurate the target nodes' trustworthiness can be recovered in the presence of WSN attacks and WSNTS attacks respectively. Unlike the trustworthiness that the trust systems need to calculate at run time, the trust accuracy and trust robustness are two performance indices that we can use to evaluate and compare different trust systems' security levels.

Trust systems do not need to compute the trust accuracy and robustness at run time.

1) Trustworthiness: From some watchdog node vi 's point of view, we define a sensor node v j 's trustworthiness in
the context of a particular behavior (e.g., data sensing or routing etc.) as the percentage of v j 's behaviors that meet
vi 's expectation among all the v j 's behaviors watched by vi in a time window N. We denote this trustworthiness as Ti j . We then define I t i j as the event to represent whether v j 's behavior is expected by vi at time slot t. I t
i j returns 1 if v j 's behavior follows vi 's expectation and returns 0 otherwise. Watchdog node's expectation is context aware. For data sensing, watchdog nodes believe their own sensing function works fine and expect to see the similar sensing value reported by the target nodes. But for routing task, watchdog nodes expect target nodes can successfully help forward packets. We calculate Ti j as:

$$T_{ij} = \frac{\sum_{t \in N \vee w_{ij}^t \neq \emptyset} I_{ij}^t}{\sum_{t \in N \vee w_{ij}^t \neq \emptyset} 1}, \qquad (6)$$

where, wt i = ∅ means the watchdog node vi actually performs watchdog task to monitor v j at time slot t.

2) Trust Accuracy and Trust Robustness: We let Itj be the event to describe a sensor node v j 's internal behavior
and draw it according to a binary distribution function Pj . Itj = 1 if v j behaves well at time slot t while Itj = 0 if v j performs attacks against WSN at t (e.g., reporting corrupted sensing data or refusing packet forwarding etc.). Watchdog node vi can sample Pj to discrete events I t i j s. We then model the accuracy of Ti j (i.e., trust accuracy) using the Kullback-Leibler divergence [30] between the probability distribution of Itj s (i.e., Pj) and the distribution of I t i j s (denoted as Qi j). KL divergence is a well known measure of the information loss when using one

information source (i.e., probability distribution) to approximate another, and hence being a good choice to measure trust accuracy. Let I be the random variable of distribution Pj and Qi j . We then can follow [30] to calculate KL divergence as:

$$D_{KL}(\mathbf{P}_j||\mathbf{Q}_{ij}) = \sum_I ln(\frac{\mathbf{P}_j(I)}{\mathbf{Q}_{ij}(I)})\mathbf{P}_j(I).$$

We use _i j to denote trust accuracy and measure it as:

$$\Lambda_{ij} = \frac{1}{D_{KL}(\mathbf{P}_j||\mathbf{Q}_{ij}) + 1}. \quad (8$$

As can be seen, _i j ∈ [0, 1] and a larger _i j indicates more accurate of the trustworthiness Ti j . If the watchdog node vi can correctly observe v j 's behaviors for all the time slots t derivative:

$$\frac{\partial^2 F}{\partial d_{ij}^2} = 4 \cdot L \cdot \epsilon + 2 \cdot \frac{1}{\alpha \cdot d_{ij}^3} > 0.$$

We thus find F(di j)'s minimal value by letting its first derivative equal to 0:

$$\frac{\partial F}{\partial d_{ij}} = 4 \cdot L \cdot \epsilon \cdot d_{ij} - \frac{1}{\alpha \cdot d_{ij}^2} = 0.$$

We solve above equation by considering di j as variant and get result di j = (4L_α) −13 . Theorem 1 has been proved. _ If we form Wj by selecting the vi with minimal F(di j), it approximately equals to optimize Eq. (10) and Eq. (11) under a constraint di j = (4L_α) −13 for vi ∈ Wj . This onstraint
makes our optimization goal well-posed and solvable. It is worth noting that, if (4L_α) −13 > r j ,
we can choose di j = r j as the optimal distance.

2) Practical Algorithm (DBP Algorithm): Although Theorem 1 gives the optimal watchdog location in theory, it is
still challenging to apply this theoretical solution to practical WSN. The reason is that, for almost sensor nodes, we cannot assume there necessarily exist some neighbour nodes located at the optimal watchdog location. In common, almost v j ∈ V may have their neighbors ∀vi ∈ Bj , di j = (4L_α) −13. To address this issue, an intuitive solution is to choose the node nearest to the theoretically optimal location as watchdog. However, this intuitive algorithm is vulnerable to discrimination attacks. That is, since the intuitive algorithm fixes the watchdog node to v j 's nearest neighbour, v j ∈ A can simply behave well to v j 's nearest node but launch WSN attacks (e.g., dropping routing packets or reporting dishonest sensing data) to the rest of v j 's neighborhood. To tackle discrimination attack while still consult the optimal location to form Wj , we propose a new distancebased probabilistic algorithm (DBP algorithm for short). This algorithm can find a set of watchdog nodes by considering those nodes' locations in a probabilistic manner. Given a target node v j , DBP algorithm selects πj · ||Bj || nodes from v j 's neighbourhood Bj to form watchdog node set Wj (i.e., ||Wj || = πj · ||Bj ||), and the selection probability of ∀vi ∈ Bj satisfies Pr[vi ∈ Wj] ∝ 1 |di j−(4L_α) −1 3 | , where || ∗ || is the size of set ∗, | ∗ | returns the absolute value of ∗ and πj ∈ (0, 1]. We prove why we choose Pr[vi ∈ Wj] ∝ 1 |di j−(4L_α) −1 3 | :
Proof: In the DBP algorithm, the watchdog node selection probability Pr[vi ∈ Wj] should be larger in case the neighbor node is closer to the optimal position (4L_α) −13 given a target node v j ∈ V. Obviously, in a polar coordinates, the target node v j 's optimal position can form a circle in which the v j is the center and (4L_α) −1 3 is the radius. The nodes have the distance (4L_α) −13 to v j at any angle are always optimal.
As di j is the distance between the target node v j and another node vi in a certain angle, |di j − (4L_α) −1 3 | can express
the distance between vi and the target node v j 's optimal position. Therefore, Pr[vi ∈ Wj] ∝ 1 |di j−(4L_α) −1 3 | can well

Algorithm 1 Distance-Based Probabilistic (DBP) Algorithm

Input: π_j, B_j, d_{ij} for $\forall v_i \in B_j$, L, ϵ, α

Output: W_j

1: $W_j \leftarrow \emptyset$

2: while $||W_j|| < \pi_j \cdot ||B_j||$ do

3: $x \leftarrow random(0, \sum_{k \in B_j} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|})$

4: if $\sum_{k=1}^{i} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|} \leq x < \sum_{k=1}^{i+1} \frac{1}{|d_{kj} - (4L\epsilon\alpha)^{-\frac{1}{3}}|}$ then

5: $W_j \leftarrow W_j \vee v_i$

6: end if

7: end while

represent that the nodes near the optimal position have a higher probability to be selected. _ DBP algorithm can resist discrimination attack due to the probabilistic selection manner and the maintenance of some watchdog node redundancy determined by πj . Algorithm 1 describes the pseudo code of our DBP algorithm runs in each sensor node v j ∈ V. There, the function random(0,_k∈Bj 1 |dkj−(4L_α) −1 3 |) returns a random float value belonging to [0,_k∈Bj 1 |dkj−(4L_α) −1 3 |].

CONCLUSION

In this paper, we take the first step to answer an important research question on whether WSNTS can still maintain

Sufficient security when the trust's basic foundations (i.e., the first-hand experiences) are minimized. We give out a very positive result to this question through theoretical analysis and extensive experiments. Our studies thus shed light a promising research direction on the design of energy-efficient WSNTS by optimizing the collection procedure of first-hand experiences.

REFERENCES

[1] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Common. ACM, vol. 47, no. 6, pp. 53–57, 2004.

[2] M. L. Das, "Two-factor user authentication in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[3] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," Ad Hoc Netw., vol. 5, no. 1, pp. 3–13, 2007.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 255–265.

[5] E. Shi and A. Perrig, "Designing secure sensor networks," IEEE Wireless Commun., vol. 11, no. 6, pp. 38–43, Dec. 2004.

[6] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor

Netw., vol. 4, no. 3, 2008, Art. ID 15.

[7] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless

sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698–1712, Nov. 2009.

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

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

[9] S. Zheng and J. S. Baras, "Trust-assisted anomaly detection and localization in

wireless sensor networks," in Proc. 8th Annu. IEEE Commun.
Soc. Conf. Sensor, Mesh, Ad Hoc Commun., Netw. (SECON), Jun. 2011, pp. 386–394.
[10] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novel approach to trust management in unattended wireless sensor networks,"
IEEE Trans. Mobile Comput., vol. 13, no. 7, pp. 1409–1423, Jul. 2014.
[11] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," IEEE Trans. Inf.
Forensics Security, vol. 8, no. 6, pp. 924–935, Jun. 2013.
[12] D. Wang, T. Muller, Y. Liu, and J. Zhang, "Towards robust and effective trust management for security: A survey," in Proc. 13th IEEE Int. Conf. Trust, Secur., Privacy Comput. Commun. (TrustCom), 2014.
[13] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proc. IEEE, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.
[14] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," Comput.
Commun., vol. 33, no. 9, pp. 1086–1093, 2010.
[15] F. G. Nakamura, F. P. Quintão, G. C. Menezes, and G. R. Mateus, "An optimal node scheduling for flat wireless sensor networks," in Proc.
4th Int. Conf. Netw., 2005, pp. 475–482.
[16] A. Salhieh, J. Weinmann, M. Kochhal, and L. Schwiebert, "Power efficient topologies for wireless sensor networks," in Proc. Int. Conf.
Parallel Process., Sep. 2001, pp. 156–163.
[17] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surv. Tuts., vol. 13, no. 4,
pp. 562–583, Oct./Dec. 2011.
[18] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 867–880, 2012.
[19] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," IEEE Commun. Surv. Tuts., vol. 11, no. 2, pp. 52–73,
Apr./Jun. 2009.
[20] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Locationcentric isolation of misbehavior and trust routing in energy-constrained
sensor networks," in Proc. IEEE Int. Conf. Perform., Comput., Commun., 2004, pp. 463–469.
[21] R. Yan, H. Sun, and Y. Qian, "Energy-aware sensor node design with its application in wireless sensor networks," IEEE Trans. Instrum. Meas., vol. 62, no. 5, pp. 1183–1191, May 2013.
[22] A. Perrig, R. Szewczyk, J. D. Tygar, V.Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless Netw., vol. 8, no.5, pp. 521–534, 2002.
[23] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Secur., Adv. Commun. Multimedia Secur., 2002, pp. 107–121.
[24] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor
networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670, Oct. 2002.
[25] R. Di Pietro, G. Oligeri, C. Soriente, and G. Tsudik, "United we stand: Intrusion resilience in mobile unattended WSNs,"

IEEE Trans. Mobile Comput., vol. 12, no. 7, pp. 1456–1468, Jul. 2013.
[26] G. Chelius, A. Fraboulet, and E. B. Hamida. (2009). WSNet: An Event- Driven Simulator for Large Scale Wireless Sensor Networks. [Online]. Available: http://wsnet.gforge.inria.fr/
[27] F. Bao, I. R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trustbased
routing and intrusion detection," IEEE Trans. Netw. Service Manage., vol. 9, no. 2, pp. 169–183, Jun. 2012.
[28] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," Int. J. Distrib. Sensor Netw., vol. 2014, Jan. 2014, Art. ID 209436.
[29] R. K. Tripathi, Y. N. Singh, and N. K. Verma, "Two-tiered wireless sensor networks—Base station optimal positioning case study," IET
Wireless Sensor Syst., vol. 2, no. 4, pp. 351–360, Dec. 2012.
[30] S. Kullback, Information Theory and Statistics. New York, NY, USA : Dover, 2012.
[31] A. J. Jerri, "The Shannon sampling theorem—Its various extensions and applications: A tutorial review," Proc. IEEE, vol. 65, no. 11,
pp. 1565–1596, Nov. 1977.
[32] A. Fraboulet, G. Chelius, and E. Fleury, "Worldsens: Development and prototyping tools for application specific wireless sensors networks," in Proc. 6th Int. Symp. Inf. Process. Sensor Netw., Apr. 2007, pp. 176–185.
[33] J. Tate, B. Woolford-Lim, I. Bate, and X. Yao, "Evolutionary and principled search strategies for sensornet protocol optimization," IEEE
Trans. Syst., Man, Cybern. B, Cybern., vol. 42, no. 1, pp. 163–180, Feb. 2012.

Author 1:

Kavuri Lakshmi Ranganadha Simha, pursuing M.Tech CSE, Newtons Institute of Engineering A.P, India

Author2:

D Rammohan Reddy , Associate professor Department of CSE, , Newtons Institute of Engineering A.P, India