HAJAR, M.S., AL-KADRI, M.O. and KALUTARAGE, H. 2020. ETAREE: an effective trend-aware reputation evaluation engine for wireless medical sensor networks. In Proceedings of *2020 Institute of Electrical and Electronics Engineers (IEEE) Communications and network security conference (CNS 2020), 29 June - 1 July 2020, [virtual conference]*. Piscataway: IEEE [online], article ID 9162325. Available from: https://doi.org/10.1109/CNS48642.2020.9162325

ETAREE: an effective trend-aware reputation evaluation engine for wireless medical sensor networks.

HAJAR, M.S., AL-KADRI, M.O. and KALUTARAGE, H.

2020

ETAREE: An Effective Trend-Aware Reputation Evaluation Engine for Wireless Medical Sensor Networks

Muhammad Shadi Hajar, M. Omar Al-Kadri, Harsha Kalutarage
School of Computing
Robert Gordon University
Aberdeen, United Kingdom
{m.hajar, o.alkadri, h.kalutarage}@rgu.ac.uk

***Abstract*—Wireless Medical Sensor Networks (WMSN) will play a significant role in the advancements of modern healthcare applications. Security concerns are still the main obstacle to the widespread adoption of this technology. Conventional security approaches, such as authentication and encryption, are able to defend against external attacks effectively. However, internally launched threats, either by compromised or selfish nodes, require further security measures to be detected. In this paper, an Effective Trend-Aware Reputation Engine (ETAREE) is proposed for WMSN. ETAREE uses a novel updating mechanism to evaluate the reputation value, which makes it effective in detecting malicious nodes. Moreover, the proposed updating mechanism of ETAREE can efficiently detect on-off attacks. ETAREE security evaluations have been presented and compared with different reputation evaluation models, demonstrating faster detection of malicious behaviours.**

***Index Terms*—Wireless Medical Sensor Networks (WMSN), security, reputation evaluation, trend-aware, internal attacks, beta distribution.**

I. Introduction

Wireless Medical Sensor Networks (WMSN) offer promising healthcare applications, ranging from monitoring physiological vital signs to providing telemedicine [1]. WMSN consist of tiny bio-sensor nodes with wireless communication capability located on the body surface, inside the body, or in the vicinity of the body. This cutting edge technology will ease patients' lives and help caregivers by alerting them for timely intervention. Due to the ad hoc nature of the WMSN, the cooperation between network's nodes is an imperative issue to ensure the operability of the network as malicious or selfish nodes may pose serious threats to the service availability.

WMSN are prone to different types of threats that affect its operation and consequently endanger the patient's life. In addition to its scarcity of resources, WMSN inherit many security vulnerabilities from Wireless Sensor Networks (WSN). Cryptographic measures provide advantageous mechanisms to ensure the confidentiality, integrity and authenticity; however, it can not be regarded as a sufficient security solution. For instance, a legitimate node, which is authenticated and may have a copy of the keys, may get compromised, and thereby it may selectively forward some packets and drop others. This significantly degrades the service quality, and can disrupt the operation of the entire network.

Attacks can be classified into internal and external according to the attack's origin. Authentication and encryption schemes are effective in defeating external attacks [2]. However, they do not satisfy the security requirements for defeating internal attacks [3]. Therefore, trust and reputation evaluation systems are introduced in the literature to detect internal attacks. They are regarded as promising measures in defending against internal attacks such as packet forwarding attacks, which can be launched by compromised or selfish nodes [4]. WMSN are susceptible to the same internal attacks of WSN; however, data in WMSN are very critical and sensitive as dropping such packets may endanger the patient's life. Packet forwarding attacks constitute a significant part of the internal attacks that WMSN may face. Below are the most common packet forwarding attacks:

- Selective Forwarding Attack: In this type of internal attacks, the compromised node drops packets intentionally based on some criteria it has. For example, it may drop packets for a particular destination or even from a particular source [5].
- Sink Hole Attack: This type of internal attacks occurs when the malicious node is able to attract all the traffic within the network and then drops all the received packets [6].
- Black Hole Attack: It is similar to selective forwarding attack. However, in black hole attack, the malicious node drops all the received packets [6].
- On-off Attack: One of the smart packet forwarding attacks where the compromised node alternately changes its behaviour between benign and malicious manners in order to keep itself undetected [7]. Hence, malicious node is regarded as trusted one while it continues to disrupt the network operation.

There are mainly two different reasons why some nodes within the network launch packet forwarding attacks. The first is when the node is got compromised and intentionally stops forwarding packets according to the malicious piece of software it has. The second is when a benign node tend to selfishly stop forwarding packets for others in order to save power. Regardless of the reason, packet forwarding attacks pose serious threats that may endanger the patient's life. For instance, the dropped packet may contain a command for an insulin pump to release a dose of insulin into the blood stream and dropping such a packet has serious consequences. Hence, an adequate technique to detect and defeat such attacks is imperative. However, any proposed scheme should be able to detect attacks as fast as possible to avoid the serious consequences of continuity of attacks. Therefore, an effective measure that defend against packets drop attacks is still an open area of research.

Many trust and reputation schemes are put forward based on beta distribution in the WSN field. However, in their current state, they do not fit WMSN due to their prolonged time in detecting malicious activities [8]. This is not acceptable from the WMSN perspective due to their critical applications. The main contribution of this paper is introducing a novel trend-aware reputation engine termed as "ETAREE", which is a modified beta distribution based reputation engine. ETAREE uses an efficient updating mechanism based on double exponential weighting with a view to respond to any change in node's behavior and speed up the process of detecting malicious nodes. Furthermore, It conforms to the resources limitations of WMSN as the reputation calculation of beta distribution based schemes is lightweight [9].

The remainder of this paper is organized into six sections as follows. Related works are given in section II. Section III presents an overview of the reputation evaluation mechanism. The reputation engine ETAREE is then introduced in section IV, followed by performance analysis and comparison results provided in section V. Finally, section VI concludes the paper.

II. Related Works

Reputation is a process to quantify the neighbors' behaviour based on previous interactions. Quantifying the reputation of nodes in the vicinity has very potential applications ranging from routing [10] to defeating threats [9]. Reputation evaluation has been widely investigated in the literature especially for E-Commerce [11]. However, more attention has to be paid for WMSN because of its critical applications.

A number of reputation evaluation schemes have been proposed in the literature for WMSN [9] and WSN [12]–[14]. Currently, different types of reputation models are used to evaluate the reputation value such as fuzzy based [15] and probability based [12]. However, probability distribution based reputation models are extensively used because of its robust mathematical foundation to represent the reputation value; moreover, it is regarded as a lightweight method [9].

Among all the probability distribution functions, beta probability distribution attracts more attention because of its simplicity and flexibility to represent different datasets with a variety of shapes by changing its parameters [16]. However, Exponential distribution and Binomial distribution are also introduced in the literature [14], [17].

To the best of our knowledge, authors in [18] are the first to introduce the beta-based reputation model. Later on, Reputation-based Framework for Sensor Networks (RFSN) [12] was introduced as a beta-based reputation framework for WSN. RFSN is built to integrate new updates into the reputation evaluation process. Those updates are obtained using a watchdog mechanism that collects cooperative and non-cooperative interactions. RFSN adopts a forgetting mechanism with a view to give more weight to recent observations. Because of the effectiveness of the probability based reputation evaluation system, many improvements are introduced in the literature that show promising results. However, to the best of our knowledge, similar updating mechanism is used in those schemes. ReTrust [9] is another beta distribution based scheme. Authors of ReTrust define a lightweight and attack resistant scheme to fit WMSN. ReTrust adopts the sliding time window concept to evaluate the reputation value, thereby it ignores any historical interactions beyond the sliding window. Further, the aging factor is redefined to be a vector where its elements' number is equal to the length of the time window and the value of those elements are exponentially decreasing to underweight earlier observations. Moreover, with a view to defeat on-off attack, authors suggest a dynamic aging factor instead of the fixed one. Authors in TWSN [19] use a different technique to evaluate the direct trust by calculating the forwarding ratio based on the accumulated successful and unsuccessful actions. Afterwards, the forwarding ratio is compared with the previous one in order to compute the fluctuation of the node behaviour, which will be used later to evaluate the direct trust using the cosine function.

On the other hand, few research in the literature adopt different types of probability distribution functions to evaluate the reputation value. Despite using different probability distribution functions, the reputation value is evaluated using the same formula of beta-based reputation models. This is because the reputation value in the beta-based schemes is defined as the expected value of the probability distribution while in other schemes, it is computed as the maximum value of the probability distribution. BDTMS [17] is a binomial distribution based reputation scheme for WSN oriented to the healthcare applications, whilst ETRES [14] uses the exponential distribution to represent the reputation value. Both BDTMS and ETRES use the same weighting mechanism to underweight old observations.

III. Reputation Evaluation

In this section, an overview of the probability based reputation model is presented.

A. The Definition of Reputation

Defining trust and reputation is still an open issue [20]. Trust can be defined as having an adequate confidence on the others' future behaviour while Reputation is the perception that others do not have any intention to change their known behaviour.

Although reputation and trust are used interchangeably sometimes in the literature, there is a difference between them. Reputation value is usually inferred from the behaviour history while calculation of trust value is a subjective expectation that may consider more factors, which are not necessarily related to the trustee. As the reputation relationship is usually built between two parties for a specific action, the first party that maintains the reputation value is referred to as a subject while the second party that performs the action is referred to as an agent [9]. Therefore, the notation *R(subject:agent,action)* is used to refer to the reputation value maintained by the subject node for an agent node. Fig. 1 illustrates the aforementioned notation and highlights how reputation-based trust could be evaluated. Actions can be any service provided by an agent to a subject such as packets forwarding, which will be the case in this paper. In such case, the subject observes the agent's behaviour and then evaluates the agent's reputation value based on the number of successful and unsuccessful actions. It is worth mentioning that the two terms behaviour and action are used interchangeably throughout this paper.

The successful and unsuccessful actions form two series where each time unit contains the number of successful and unsuccessful actions, respectively. These two series are used to update the reputation value periodically. The updating mechanism allows nodes in the network to detect malicious, compromised, selfish or even faulty nodes and thereby exclude them from any further cooperation for example.

B. Bayesian Reputation Model

The reputation value maintained by the subject represents a belief that the subject predicts the agent's future behaviour based on it in a manner that reduces the uncertainty. The Bayesian reputation model assumes that the behaviour of the agent can be estimated based on a probability distribution. The expected value of the probability distribution represents the reputation value, which gets updated once new observations are available using Bayes' theorem [8]. Therefore, the updated (posterior) parameters of the probability distribution function is calculated by adding the previous (prior) version of the parameters to the current observations.

C. Beta Distribution Based Reputation Model

As the actions monitored by the subject have two different states (forwarded or dropped), these observations could be regarded as a sequence of trials that have binary outcomes *(Successful, Unsuccessful)*, which form a binary space of disjoint elements. Therefore, the binomial Bayesian reputation system can be modeled using a Beta Probability Density Function (PDF) [21].

IV. ETAREE Reputation Evaluation Model

In this section, an Effective Trend-Aware Reputation Evaluation Engine (ETAREE) for WMSN is proposed. ETAREE is a novel reputation evaluation model based on double exponential weighting.

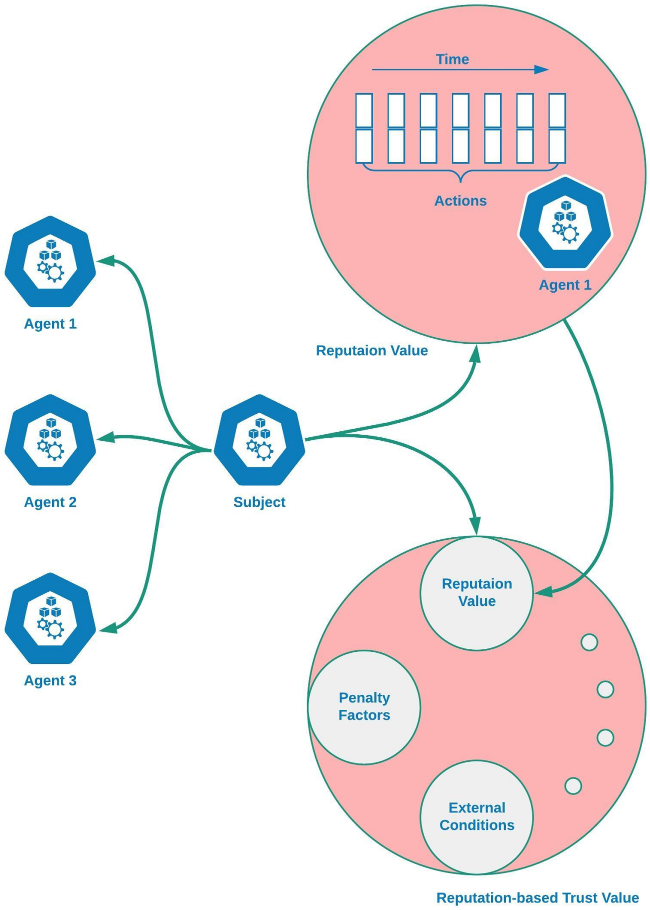


Fig. 1. Reputation and Trust

A. Motivation

Each action is done by trustee represents a Bernoulli trial with two possible outcomes. Beta distribution provides a lightweight computational method to evaluate the posterior probability based on a conjugate prior compared with Bayesian inference. Updating the beta model when new observations are available is more efficient than Bayesian inference. However, as the reputation value evaluated using beta distribution represents a long-term value, it takes long time to detect malicious behaviour [8]. This behaviour does not fit the security requirements of WMSN because of the critical application they provide. Slowness in detecting malicious nodes affects the patient's health negatively and may threaten the patient's life.

B. Beta-based Reputation Evaluation

Beta probability distribution provides a robust basis for reputation evaluation on the theory of statistics [18]. The beta probability density function, which is defined in Eq. 1, is a continuous probability distribution of the probability variable p_x over the interval [0,1]. It is parameterized by α and β, which get updated based on the binary outcomes of the observed actions.

$$f(p_x|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p_x^{\alpha-1}(1-p_x)^{\beta-1}$$
$$where \begin{cases} 0 \leq p_x \leq 1 \\ \alpha > 0 \\ \beta > 0 \end{cases} \tag{1}$$

There are two restrictions for Eq. 1. The first is $p_x \neq 0$ if $\alpha < 1$, and the second is $p_x \neq 1$ if $\beta < 1$. The expected value of the Eq. 1 represents the reputation value and is defined in Eq. 2.

$$\begin{aligned} Rep_{ij} &= E(p_x) \\ &= \frac{\alpha}{\alpha+\beta} \end{aligned} \tag{2}$$

where Rep_{ij} represents the reputation value maintained by subject i for the agent j, $E(p_x)$ is the expected value of the beta distribution, x represents the outcome of successful actions, α and β are the probability distribution function shape parameters and they represent the updated versions of the successful and unsuccessful actions between the subject i and the agent j, respectively.

Once the system is initialized, it is expected that no observations are obtained, thereby it is important to initialize the reputation value. Authors in [12] suggest the following initial value when there is no prior knowledge:

$$Rep_{ij} = E[uni(0,1)] \tag{3}$$

This means when no observations are available, the probability variable is uniformly distributed over the interval [0,1] and the initial reputation value is 0.5, and thereby the reputation value is evaluated using Eq. 4.

$$Rep_{ij} = \frac{\alpha+1}{\alpha+\beta+2} \tag{4}$$

C. Traditional Beta Updating Mechanism

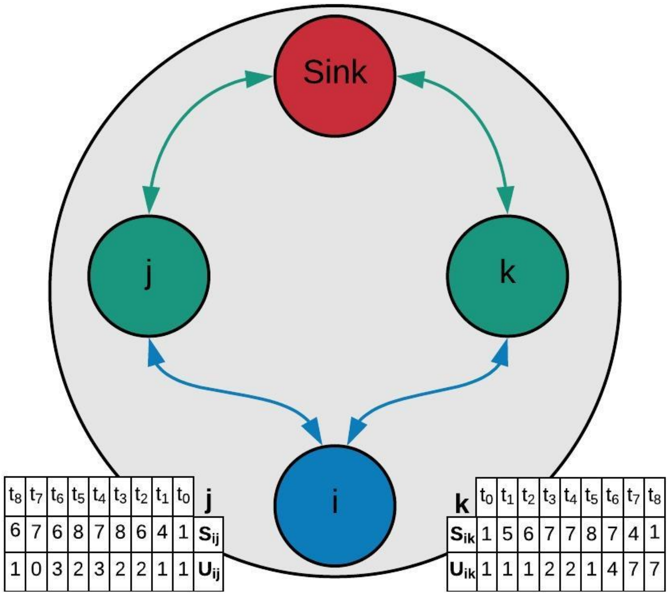
Let us consider the Body Sensor Network (BSN) illustrated in Fig. 2. This two-hop star topology represents the first tier of communication of WMSN. Node i is not in the direct communication of the sink node. Nodes j and k have the capability to relay packet for end nodes such as i. Therefore, subject i evaluates agents j and k for the packet forwarding action. Let s be the number of observations of successful actions and u to be the number of observations of unsuccessful actions in the time unit t. Thereby the reputation value of the agent j, which is maintained by the subject i is given by Eq. 5:

$$\begin{aligned} Rep_{ij} &= E[\frac{\Gamma(\alpha+s+\beta+u)}{\Gamma(\alpha+s)\Gamma(\beta+u)} p_x^{\alpha+s-1}(1-p_x)^{\beta+u-1}] \\ &= E[Beta(\alpha+s, \beta+u)] \end{aligned} \tag{5}$$

It is clear that the updated reputation value can be obtained by updating the two parameters α and β as shown in the two equations below:

$$\alpha_t = \alpha_{t-1} + s \tag{6}$$

$$\beta_t = \beta_{t-1} + u \tag{7}$$



t_8	t_7	t_6	t_5	t_4	t_3	t_2	t_1	t_0	j
6	7	6	8	7	8	6	4	1	S_{ij}
1	0	3	2	3	2	2	1	1	U_{ij}

k	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8
S_{ik}	1	5	6	7	7	8	7	4	1
U_{ik}	1	1	1	2	2	1	4	7	7

Fig. 2. Network setup

The aforementioned updating mechanism gives equal weight to all past observations, and thus it is not able to reflect recent changes in behaviour. Another issue is that α and β are accumulated over the time and thereby more memory would be required, which violates the resources constraints of WMSN. Therefore, longevity factor λ, also known as forgetting factor or aging factor, is introduced. Longevity factor is a decay factor widely used in the literature to give more weight to the new observations [12], [14], [18].

$$\alpha_t = \lambda.\alpha_{t-1} + s \tag{8}$$

$$\beta_t = \lambda.\beta_{t-1} + u \tag{9}$$

where $0 \leq \lambda \leq 1$. This updating technique that gives more weight to the recent observations and decreases the weight slowly over the time is called Single Exponential Smoothing (SES). Fig. 3 shows how beta-based reputation engine reflects the reputation value using different longevity weights for benign and malicious nodes.

D. Trend-Aware Updating Mechanism

The reputation value evaluated by the beta-based reputation model responds slowly to changes in the agent's behaviour. Fig. 4 depicts how beta-based reputation model responds to a simple change in agent's behaviour. A sequence of 10 time units where the agent provides successful actions followed by another 10 time units of unsuccessful actions. It takes 10 time units for beta-based reputation model without longevity weight to reach the threshold, which is set to 0.5, while it takes 7 time

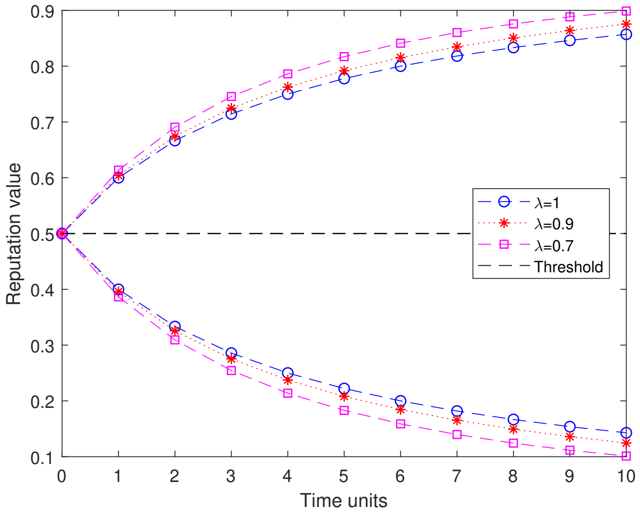


Fig. 3. The beta-based reputation model with different longevity weights for benign and malicious nodes

units for the beta-based reputation with 0.9 longevity weight to exceed the threshold value. Adversary can take advantage of the long detection period to destroy the network or even to launch more complicated attacks such as on-off attack. Note that using small longevity factor is not recommended because the subject forgets the behaviour history quickly, and consequently allows the adversary to launch attacks leveraging its reputation value.

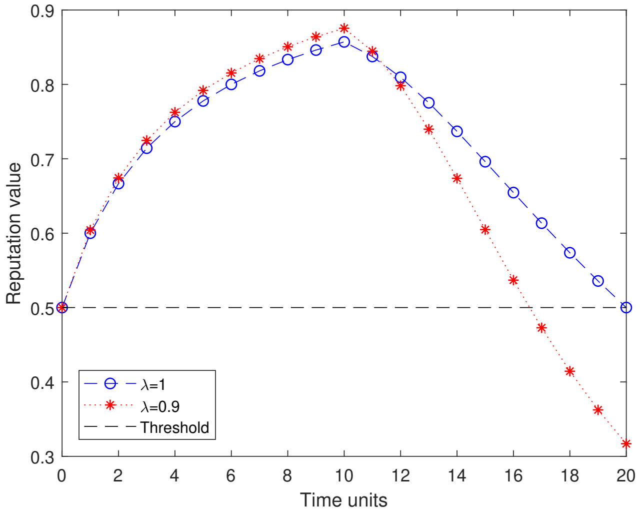


Fig. 4. The beta-based reputation model for 10 good observations followed by 10 bad ones

1) Double Exponential Weighting: In order to reduce the time required to detect malicious behaviour of the beta-based reputation model, and thereby enhance the detection rate, the trend of the agent's behaviour has to be considered. ETAREE considers the exponentially smoothed difference between two subsequent time units of the agent's behaviour by evaluating the additive slope of the successful and unsuccessful series. Therefore, ETAREE uses double exponential weights λ_1 and λ_2 as opposed to a single weight in models proposed in the literature. Taking into account that the difference between two subsequent time units is always one, Eq. 10-13 show the proposed updating mechanism where the levels (beta distribution shape parameters) α_t and β_t are updated by considering the slope between the two subsequent time units, which represents the difference between observations for each series.

$$\alpha_t = \lambda_1(\alpha_{t-1} + b_{t-1}) + (1-\lambda_1)s_t \tag{10}$$

$$b_t = \lambda_2(\alpha_t - \alpha_{t-1}) + (1-\lambda_2)b_{t-1} \tag{11}$$

$$\beta_t = \lambda_1(\beta_{t-1} + d_{t-1}) + (1-\lambda_1)u_t \tag{12}$$

$$d_t = \lambda_2(\beta_t - \beta_{t-1}) + (1-\lambda_2)d_{t-1} \tag{13}$$

where b_t and d_t are the slopes at the time unit t for the successful and unsuccessful series, respectively, λ_1 and λ_2 are the weighting coefficients and ($0 \leq \lambda_1 \leq 1$, $0 \leq \lambda_2 \leq 1$), s_t and u_t are the number of observations at the time unit t of the successful and unsuccessful actions, respectively.

Slopes b_t and d_t may have negative values depending on the series, whereas reputation value must be positive within the interval $[0,1]$. Therefore, the Eq. 10 and Eq. 12 are written as follows:

$$\alpha_t = \alpha_t^+ \tag{14}$$

$$\beta_t = \beta_t^+ \tag{15}$$

where α_t^+ and β_t^+ are the positive part of the real value and are defined as:

$$f_t^+ = \frac{|f_t| + f_t}{2} \tag{16}$$

2) Reputation Engine Initializing: There are two points to consider upon system initialization. The first is the initial reputation value, which has been discussed earlier to overcome the case where no observations are available. The second is related to our proposed reputation engine as computing the slope needs at least two time units of observations.

The reputation value evaluated using the Eq. 4 considers adding the value 1 to both α_t and β_t to ensure that the initial reputation value is 0.5 at the beginning; further, this formula is usually adopted by schemes that consider the reputation over a predefined time window, because it protects the system from division by zero problem when no observations are available for the whole time window. On the other hand, adding 1 to the numerator and 2 to the denominator will influence the reputation value especially when the number of observations is limited as depicted in Fig. 5

In ETAREE, the reputation value is evaluated using the formula in Eq. 2, which is simpler and does not influence

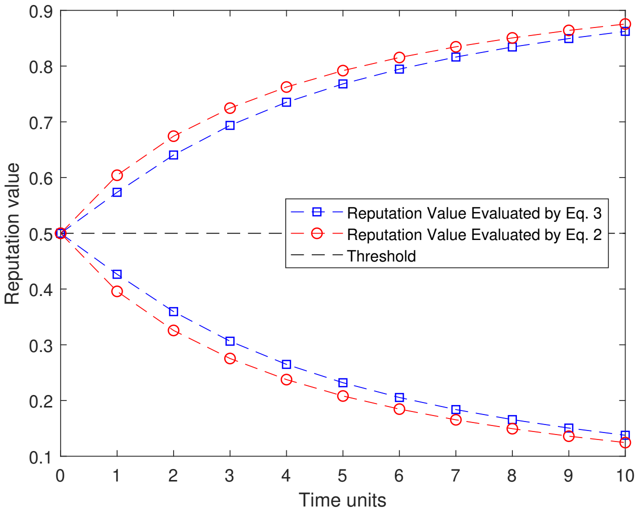


Fig. 5. The difference between reputation values evaluated using Eq. 2 and Eq. 4 over 10 time units

the reputation value. However, to overcome the aforementioned problems and assign the proper initial value, ETAREE assumes a predefined time unit t_0 where the number of successful and unsuccessful actions are set to 1 as illustrated in Fig. 2.

Assuming that ETAREE is applied from the origin where no actual observations are available except the predefined observations in the time unit t_0, the initial slopes' values will be as follows:

$$b_{t_0} = d_{t_0} = 0 \tag{17}$$

$$b_{t_1} = s_{t_1} - s_{t_0} \tag{18}$$

$$d_{t_1} = u_{t_1} - u_{t_0} \tag{19}$$

where s_t and u_t are the number of observations in the time unit t for both successful and unsuccessful actions, respectively.

V. Evaluation

In this section, the security effectiveness of ETAREE reputation engine is presented. In order to assess our proposed reputation engine, ETAREE has been implemented using MATLAB platform. Since RFSN [12] is considered the benchmark scheme [14], ETAREE has been contrasted with it. Moreover, a comparative analysis with [19] and [9] is presented. The results show that ETAREE is more dynamic and can reflect behavioural changes into the reputation value faster than other schemes. Moreover, ETAREE is able to detect low packets drop rates compared with other schemes. Hence it is more efficient to defend against malicious behaviour such as packets dropping in WMSN.

As discussed earlier, all nodes are initially regarded as good nodes and assigned the same reputation value 0.5 by setting one successful action and one unsuccessful action at the time unit t_0. Choosing the same value for successful and unsuccessful actions is mandatory to initialize the reputation value to 0.5; however, the bigger the value is, the more influence it has on the next reputation values.

BSN consists of sensor nodes where one of them acts as a sink. According to [22], BSN is a two-hop star topology where all sensor nodes send their sensed medical data to the sink. In this star topology, nodes, which are in the direct communication with the sink, have to relay packets for others. Therefore, to assess reputation in such a network topology, two different approaches are considered, centralized and distributed, where both have their pros and cons. ETAREE is a distributed reputation engine where an instance of it is installed in each node. Our experiments adopt the network topology illustrated in Fig. 2, where node i is not in a direct communication with the sink node; therefore, it has to send its packets to either node j or node k in order to be relayed to the sink node. Subject i maintains reputation values for both agents j and k.

Taking into account the aforementioned factors, subject i evaluates the reputation of agent j and/or agent k in the following scenarios. Table I shows the used parameters of each scheme where the same longevity factor is used to allow fair comparison. Moreover, we adopt the values of the schemes' parameters as declared in each scheme publication where available. Regarding ETAREE, λ_1 is set to 0.8 as it presents the longevity factor, λ_2 is set to 1 as in WMSN our highest priority is to detect malicious behaviours as fast as we can. The threshold is set to 0.5 to differentiate between malicious and benign nodes as this value is widely adopted in the literature. Note that all the evaluated reputation values are the direct reputation values as the indirect reputation evaluation is out of the scope of this paper.

TABLE I
Performance Analysis Parameters

Scheme	Performance Analysis Parameters
RFSN [12]	λ=0.8
ReTrust [9]	ϕ=0.9, TW(Time Window)=6 time units
TWSN [19]	$\alpha = 0.9$, $\beta = 0.8$
ETAREE	λ_1=0.8, λ_2=1.0

A. Scenario 1

In the first scenario, we assume that the subject i is evaluating two different agents j and k. one of them is behaving good while the second one is behaving bad throughout the evaluation process. Agents j and k are initially assigned the same reputation value of 0.5 as the time unit t_0 is preset to (1,1) actions. A threshold value is set to 0.5. Fig. 6 illustrates the reputation evaluation of ETAREE in contrast with RFSN, ReTrust and TWSN.

The results show that all the evaluated schemes are developing the reputation value gradually for both benign and malicious agents over the time. However, ETAREE reflects the best performance among them for both good and malicious agents by giving the lowest reputation value for the malicious agent and the highest reputation value for the good agent, thereby it converges to 0 or 1 better than other schemes. While

RFSN and TWSN performs closely, ReTrust, in the first five time units, performs in a similar way; however, when the first time window is formed as the Time Window (TW) is set to 6, ReTrust tends to underestimate the reputation value of the good agent and overestimate the reputation value of the malicious agent.

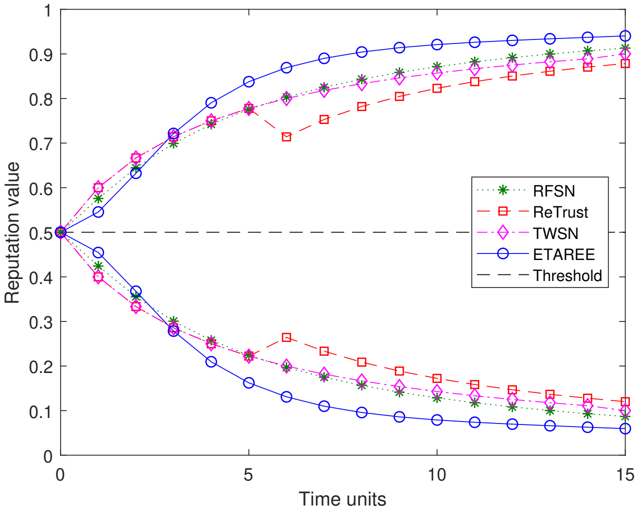


Fig. 6. The reputation evaluations for good and malicious nodes

B. Scenario 2

The second scenario depicts how each scheme responds to a sudden change in agent's behaviour. We assume that the subject i is evaluating agent's j behaviour. Agent j is behaving in a good manner in the phase I between the time units 1 and 15, then suddenly it behaves maliciously. As in the first scenario all schemes are initialized with the same reputation value and the same threshold. Our proposed scheme ETAREE is compared with RFSN, ReTrust and TWSN.

Fig. 7 presents the reputation evaluation of the second scenario. All schemes demonstrate a similar behaviour to the first scenario during the first phase. However, during the malicious phase, RFSN and ReTrust show approximately similar reactions to the malicious behaviour, although ReTrust shows faster detection as it needs 5 time units to pass the threshold. TWSN fails to detect the attack in the malicious phase as it converge to just above 0.6 at the time unit 25. RFSN and ReTrust converge to around 0.3 and 0.2, respectively. On the other hand, our proposed scheme ETAREE reaches the threshold within 4 time units and converge to 0 within 6 time units. Moreover, it is clear that while the malicious agent continues its bad behaviour, ETAREE, unlike other schemes, tends to decrease the reputation value further over the time, which allows it to detect attack for even lower threshold.

C. Scenario 3

In this scenario, the on-off attack will be evaluated where the malicious node is aware that the punishment for any malicious activities is temporary as it is able to redeem itself and get back again to the network by showing good behaviour alternately. During the reputation evaluation process, Node k is running an on-off attack that contains two on(s) and two off(s) periods, and the attack cycle is 10 time units. During the on phase, node k acts maliciously and drops packets that it is expected to forward them. Our proposed scheme ETAREE is contrasted with RFSN, ReTrust and TWSN for the same initial reputation value and threshold.

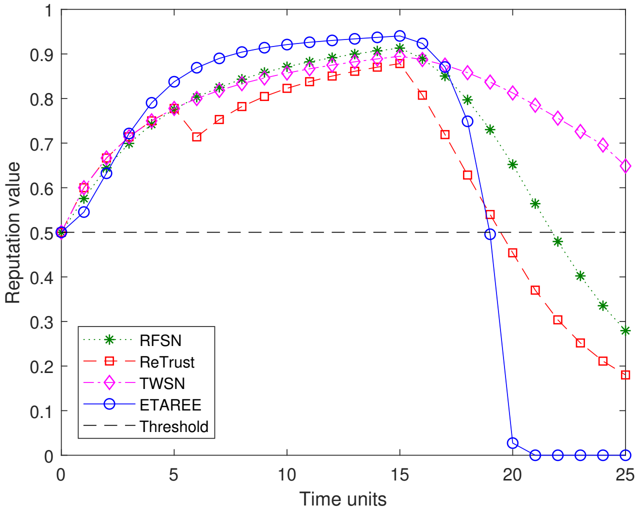


Fig. 7. The reputation evaluations when an agent changes its behaviour from good to bad

The reactions to on-off attack for all the aforementioned schemes are illustrated in the Fig. 8. In the first phase where the agent is acting in a cooperative manner, all schemes demonstrate similar behaviour. One point to highlight in this phase is, ETAREE is the only scheme that is able to converge to 1 and reflect the actual reputation value among others. During the first on period, it is obvious how RFSN and TWSN are not able to detect the attack, while ReTrust reaches the threshold after 3 time units. On the other hand, ETAREE is able to exceed the threshold with the same time units of ReTrust. Afterwards, ETAREE shows a very dynamic behaviour in contrast with other schemes by reflecting the agent's good behavior. However, this dynamicity in reflecting cooperative behaviour does not prevent ETAREE from detecting malicious agent, which is running the on-off attack during the second on period. By the end of the second on period, the reputation value of RFSN and ReTrust converge to around 0.2 while TWSN fails to detect the attack as it converges to just above 0.6. On the other hand, ETAREE converges to 0 after just 5 time units, which allows it to detect attacks even for lower threshold.

D. Scenario 4

In this experiment, we evaluate the detection speed of the aforementioned schemes for different packets drop rates. The second scenario is run multiple times by decreasing the packets

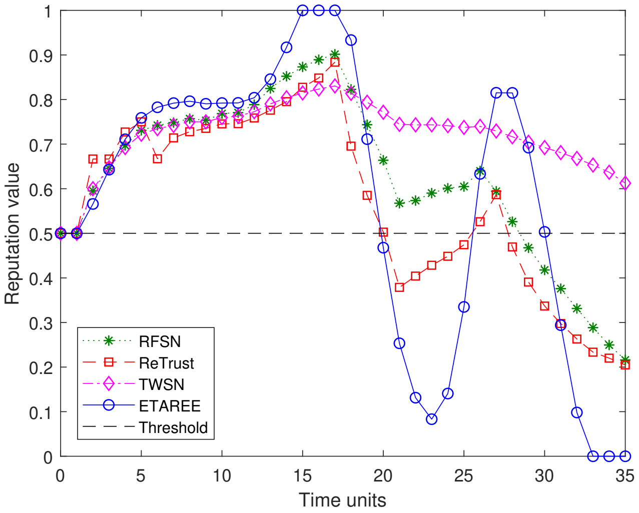


Fig. 8. The reputation evaluations under on-off attack

drop rate by 10% each time. The same initialization and threshold are used. Fig. 9 illustrates the required time for each scheme to detect the attack.

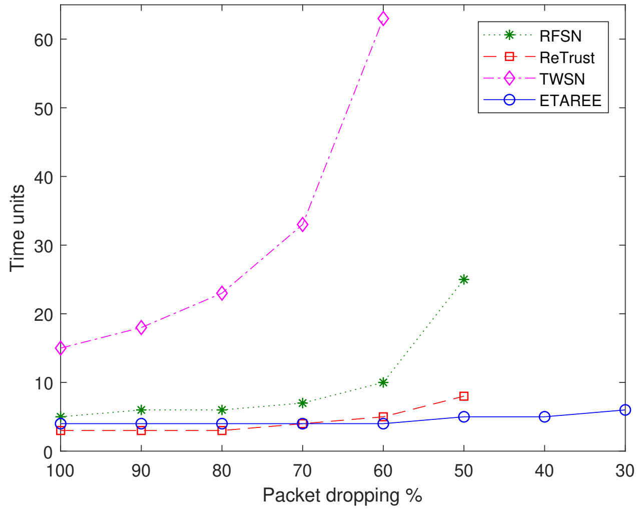


Fig. 9. The attack detection speed

TWSN shows longer time to detect the attack with a remarkable rise each time the packets drop rate decreases. Other schemes, including ETAREE, detect attacks by approximately the same time units at the beginning; however, ETAREE shows better performance by decreasing the packets drop rate. On the other hand, by decreasing the drop rate, TWSN fails to detect attacks when the rate is less than 60%, while RFSN and ReTrust are still able to detect attacks down to 50%. Most importantly, ETAREE is the only scheme that is able to detect attacks with packets drop rate as low as 30%, which makes it more effective and robust comparatively.

VI. Conclusion

Reputation evaluation measures are considered an effective method to defend against packet forwarding attacks and detect malicious or selfish activities. Beta-based reputation model offers a promising solution; however, it takes a prolonged time to detect compromised or selfish nodes. Our proposed reputation engine, ETAREE for short, presents a suitable solution. In ETAREE, we adopt a double exponential weighting updating mechanism with a view to make beta-based reputation evaluation model faster in detecting malicious activities. ETAREE demonstrates promising results compared with RFSN, ReTrust and TWSN. On the other hand, adversary could take advantage of the dynamicity of reflecting behavioural changes from malicious to benign to launch more sophisticated attacks. Moreover, ETAREE still needs further evaluations within a trust system that considers indirect recommendations from other nodes in the vicinity, which will be part of our future research.

References

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, “Wireless body area networks: A survey,” *IEEE Communications surveys & tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[2] M. Masdari and S. Ahmadzadeh, “Comprehensive analysis of the authentication methods in wireless body area networks,” *Security and Communication Networks*, vol. 9, no. 17, pp. 4777–4803, 2016.

[3] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, “Btres: Beta-based trust and reputation evaluation system for wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 59, pp. 88–94, 2016.

[4] R. Feng, X. Xu, X. Zhou, and J. Wan, “A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory,” *Sensors*, vol. 11, no. 2, pp. 1345–1360, 2011.

[5] S. S. Javadi and M. Razzaque, “Security and privacy in wireless body area networks for health care applications,” in *Wireless networks and security*. Springer, 2013, pp. 165–187.

[6] P. Niksaz and M. Branch, “Wireless body area networks: attacks and countermeasures,” *International Journal of scientific and engineering research*, vol. 6, no. 19, pp. 565–568, 2015.

[7] N. Labraoui, M. Gueroui, and L. Sekhri, “On-off attacks mitigation against trust systems in wireless sensor networks,” in *IFIP International Conference on Computer Science and its Applications*. Springer, 2015, pp. 406–415.

[8] M. E. Moe, B. E. Helvik, and S. J. Knapskog, “Comparison of the beta and the hidden markov models of trust in dynamic environments,” in *IFIP International Conference on Trust Management*. Springer, 2009, pp. 283–297.

[9] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, “Retrust: Attack-resistant and lightweight trust management for medical sensor networks,” *IEEE transactions on information technology in biomedicine*, vol. 16, no. 4, pp. 623–632, 2012.

[10] Y. Stelios, N. Papayanoulas, P. Trakadas, S. Maniatis, H. C. Leligou, and T. Zahariadis, “A distributed energy-aware trust management system for secure routing in wireless sensor networks,” in *International Conference on Mobile Lightweight Wireless Systems*. Springer, 2009, pp. 85–92.

[11] F. Hendrikx, K. Bubendorfer, and R. Chard, “Reputation systems: A survey and taxonomy,” *Journal of Parallel and Distributed Computing*, vol. 75, pp. 184–197, 2015.

[12] S. Ganeriwal and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” in *Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks*. ACM, 2004, pp. 66–77.

[13] N. Labraoui, M. Gueroui, and L. Sekhri, “A risk-aware reputation-based trust management in wireless sensor networks,” *Wireless Personal Communications*, vol. 87, no. 3, pp. 1037–1055, 2016.

[14] J. Zhao, J. Huang, and N. Xiong, “An effective exponential-based trust and reputation evaluation system in wireless sensor networks,” *IEEE Access*, vol. 7, pp. 33 859–33 869, 2019.

[15] J. Hossein, R. Mohammad *et al.*, “A fuzzy fully distributed trust management system in wireless sensor networks,” *International Journal of Electronics and Communications*, vol. 9, no. 17, pp. 1–10, 2016.

[16] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, “Trust management system in wireless sensor networks: design considerations and research challenges,” *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2015.

[17] W. Fang, C. Zhu, W. Chen, W. Zhang, and J. J. Rodrigues, “Bdtms: Binomial distribution-based trust management scheme for healthcare-oriented wireless sensor network,” in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 382–387.

[18] A. Josang and R. Ismail, “The beta reputation system,” in *Proceedings of the 15th bled electronic commerce conference*, vol. 5, 2002, pp. 2502–2511.

[19] V. B. Reddy, S. Venkataraman, and A. Negi, “Communication and data trust for wireless sensor networks using d–s theory,” *IEEE Sensors Journal*, vol. 17, no. 12, pp. 3921–3929, 2017.

[20] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, “Trust management system in wireless sensor networks: design considerations and research challenges,” *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2015.

[21] A. Jøsang and W. Quattrociocchi, “Advanced features in bayesian reputation systems,” in *International Conference on Trust, Privacy and Security in Digital Business*. Springer, 2009, pp. 105–114.

[22] “Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks,” *IEEE Std 802.15.6-2012*, pp. 1–271, Feb 2012.