Abstract—Wireless ad-hoc networks are becoming popular due to the emergence of the Internet of Things (IoT) and cyber-physical systems (CPS). Due to the open wireless medium, secure routing functionality becomes important. However, the current solutions focus on a constrain set of network vulnerabilities and do not provide protection against newer attacks. In this paper, we propose SCOTRES — a trust-based system for secure routing in ad-hoc networks which advances the intelligence of network entities by applying five novel metrics. The energy metric considers the resource consumption of each node, imposing similar amount of collaboration and increasing the lifetime of the network. The topology metric is aware of the nodes’ positions and enhances load-balancing. The channel-health metric proposes tolerance in periodic malfunctioning due to bad channel conditions and protects the network against jamming attacks. The reputation metric evaluates the cooperation of each participant for a specific network operation, detecting specialized attacks, while the trust metric estimates the overall compliance, safeguarding against combinatorial attacks. The theoretic analysis validates the security properties of the system. Performance and effectiveness are evaluated in the NS2 simulator, integrating SCOTRES with the DSR routing protocol. Similar schemes are implemented using the same platform in order to provide a fair comparison. Moreover, SCOTRES is deployed on two typical embedded system platforms and applied on real cyber-physical systems for monitoring environmental parameters of a rural application on olive groves. As is evident from the above evaluations, the system provides the highest level of protection while retaining efficiency for real application deployments.

Index Terms—CPS, IoT, Secure routing protocols, WSN.

I. INTRODUCTION

The evolution of the Internet of Things (IoT) motivates the deployment of intelligent cyber-physical systems (CPS) that utilize wireless networking. The market value of industrial settings was $157.05 million in 2016 and it is expected to grow at a compound annual growth rate (CAGR) of 33.3% from 2016 to 2021 [1]. According to the United Nations Environment Programme and the International Fund for Agricultural Development [2] around 2.5 billion people live from agricultural production systems. Research and governmental initiatives try to increase productivity and consumer’s safety by applying IoT technologies to monitor weather and crop growth [3] and CPS to manage production systems, like watering [4] and spraying pesticides with UAVs [5].

In such wireless ad-hoc networks, each entity relies on its neighbors to carry its messages and successfully communicate with all participants. Due to the open medium and the dynamic entry of new nodes to these networks, routing protocols must establish trust relationships to avoid malicious nodes.

Trust-based schemes are used in wireless networking to provide secure routing functionality. Reputation [6] is formed by a node’s past behavior and reveals its cooperativeness. In secure routing, reputation mainly evaluates the routing and forwarding, the use of encryption and authentication mechanisms, and the proper transmission of acknowledgements per transmitted packet. Trust [6] is the level of confidence that an entity holds about others. It is the aggregation of all reputation values that the entity holds for another participant. A node with high reputation values is considered trustworthy. Legitimate nodes depend mostly on trustworthy entities to accomplish communication tasks. On the other hand, low reputation can reveal selfish or malicious entities and is used for intrusion detection. Legitimate nodes try to avoid disreputable entities and do not serve their traffic.

Many trust-based systems have been utilized to achieve secure routing [7]. Each one of them is evaluated under specific ad hoc applications and tackles a constraint set of security threats. Six of the most representative state-of-the-art systems are described below.

The Semi-Distributed Reputation-based Intrusion Detection System for mobile ad-hoc networks (S-D RepIDS) [8] implements many novel reputation metrics for secure routing and is tolerant to failures due to traffic congestion. AODV Reputation EXtension (AODV-REX) [9] adopts a multi-layer model. The privacy of the recommender is protected by aggregating the direct and indirect reputation values. The recommendations are encapsulated in the underlying protocol’s routing messages to preserve performance. AODV-REX proposes the virtual lengthen of a path to punish misbehavior. In contrast to the rest secure routing schemes, the Reputation based Framework for Sensor Networks (RFSN) [10] evaluates both the node’s routing cooperativeness and the reported sensed variables (e.g. temperature). In the Trusted based Routing using Dominating Set Approach (TRDSA) [11] only a set of trusted nodes with sufficient remaining energy need to operate in promiscuous mode and capture malicious activity, reducing the overall energy consumption. Expected
Foreworded Counter (EFW) [12] combines cross network-layer observations. The network-layer module observes the routing protocol’s functionality, as in most relevant schemes, and estimate the forwarding or dropping probability of a node. Additionally, MAC-layer measurements about the wireless link quality are considered to select reliable and high performance paths. The Secure Resilient Reputation-based Routing (SR3) [13] combines a reinforced random walk algorithm with reputation.

These systems target limited sets of security vulnerabilities and attacks [14]. While the basic malfunctioning (e.g. packet drop or avoid routing participation) is efficiently detected by trust systems, there still remain several network aspects that are not properly handled, like overburden or isolate distant nodes [15], [16], [17], [18].

This work introduces the Self-Channel Observation Trust and REputation System (SCOTRES) – a novel system for secure routing in wireless ad-hoc networks and CPS. Instead of adopting features from heavy reputation-based schemes, the proposed system exploits the knowledge that each node already possesses about the network. The protocol aims to maximize the knowledge that can be inferred about the network from the data that a node already processes. For this purpose, SCOTRES utilizes efficient mechanisms that retain networks security and performance. The authors suggest that each node should invest more resources in achieving a robust individual reasoning process in order to minimize wrong decisions and the amount of data that has to be exchanged among the nodes, like the remaining node energy. This work provides evidence that a core portion of the required knowledge can be efficiently mined from the data that each node already possesses.

SCOTRES is a novel trust management scheme and counters the abovementioned routing attacks. It includes three innovative metrics:
- An efficient energy metric that protects low-energy or overloaded nodes from power dissemination, increasing the network’s lifetime
- A novel topology metric that protects topology-significant nodes and enhances load-balancing
- A channel-health metric that estimates the channel state between the nodes and avoid jamming areas

and two core reputation and trust metrics that integrate the state-of-the-art features in the secure routing domain with a few new ideas:
- A core reputation metrics that evaluates specific network operations and acknowledges reputable nodes
- A trust metrics that integrates the reputation values of all examined operations, identifying the malicious nodes and preserves the legitimate nodes private ratings.

The paper is organized as follows: In section 2, related studies on threats and protocols for secure routing are referred indicated. In section 3, the SCOTRES metrics are detailed. In section 4, theoretical analysis is provided. In section 5, the security and performance of SCOTRES are analyzed and compared with other known relevant systems in the Network Simulator 2 (NS2). In section 6, SCOTRES is applied on real embedded systems that implement a rural application. Finally, section 7 concludes.

II. RELATED WORK

A. Threats and attacks

Routing protocols fail to protect the network against selfish and malicious activity. Surveys of routing attacks in ad-hoc networks are presented in [14], [15], [19], [20], [21].

For forwarding, a flooding attacker exhausts the resources of the network and its underlying nodes (e.g. DoS, inject arbitrary packets). Blackhole and grayhole attacks discard all or selective parts of the forwarding packets respectively. In sleep deprivation, the malicious node interacts with other nodes in a manner that appears to be legitimate, while keeping them out of the power-conserving sleep mode. Other threats on packets include modification, interruption and replay.

For routing, link spoofing attackers advertise fake routing information (e.g. optimal paths) in order to avoid or impose their participation and then perform the attacks on forwarding. In wormhole attacks a pair of attackers, which communicate through a private high speed network, collide to record packets at one location and replay them at another location of the network. In colluding misrelay, a pair of neighboring attackers conspire to avoid participating in a route. In routing table poisoning, the attacker advertises false routing information (i.e. nonexistent paths, loops, false link break, and HELLO flooding) to harm the nodes’ routing capability.

Trust schemes are integrated with routing protocols as a defense mechanism. They prevent attacks on forwarding and link spoofing as they detect and negatively rank the misuse and discarding of a packet. Trust systems do not deal with wormhole attacks. However, countermeasures (e.g. [22], [23]) could be integrated, providing a more robust intrusion detection mechanism. Moreover, trust schemes do not deal with colluding misrelay attacks directly. Still, as the two nodes do not participate in routes as intermediate nodes, they cannot gain positive ratings from traffic forwarding. Thus, they are not able to make requests either. Routing poisoning is countered by evaluating the positive contribution on routing.

Nevertheless, these schemes can then become the new target of more sophisticated attacks. Survey of attacks and defense techniques for trust systems are conducted in [24], [25]. They are categorized in terms of identity-, ballot-, social- and topology-based threats and attacks.

To counter identity-based attacks (i.e. impersonation or Sybil attacks), in most relevant systems, it is assumed that a secure underlying mechanism is applied (e.g. [26], [27]), which provides authentication and confidentiality network-wide. Ballot-based attacks are countered by robust ranking and recommendation mechanisms. In order to reduce the effect of social-based attacks, a robust reasoning process and a ranking policy based mostly on direct knowledge and restrictive use of indirect knowledge are imposed. Topology-based attacks have not been extensively examined and the current systems provide no specific security treatment.

Moreover, due to the open medium, wireless
communications are vulnerable to jamming attacks, which significantly degrade the network’s performance. A survey of jamming attacks and countermeasures is reported in [16]. The accurate detection of the jammer is challenging, while precision is also significant [28]. Some of these techniques only detect some types of jamming attacks while others produce high false positives. After detection, recovery countermeasures are performed, like channel hopping and spatial retreat, based on the type of the jamming attack. However, such techniques are not always applicable, especially in wireless sensor networks (WSNs) where the nodes may have constrained communication capabilities.

B. Secure routing protocols

In this study, we concentrate on six representative secure routing protocols: TRDSA, EFW, SR3, S-D RepIDS, AODV-REX, and RFSN. TRDSA, EFW, and SR3 utilize basic reputation mechanisms for their core deductive components. S-D RepIDS, AODV-REX, RFSN, and SCOTRES apply more robust reasoning processes for evaluating direct knowledge and making recommendations.

Information regarding the remaining energy and traffic congestion is also processed. TRDSA’s routing operation takes into account the energy consumption. S-D RepIDS provides protection in congested periods. SR3 reduces congestion traffic due to the random nature of the random walk algorithm. The MAC-layer measurements of EFW assigns low communication reliability to the overloaded links, routing the traffic through alternative paths. SCOTRES protects the network in all these cases. Moreover, TRDSA, SR3 and SCOTRES perform load-balancing mechanisms to enhance performance and increase the longevity of the nodes. EFW and SCOTRES are the only systems that implement fault tolerance mechanisms to mitigate the effect of jamming attacks. SCOTRES is efficient in terms of energy consumption and performance, and protects the network against most threats. It achieves sufficient load-balancing and retains the nodes’ energy dissipation. The overall security of SCOTRES surpasses the protection that is provided by current solutions.

III. SCOTRES

Dynamic Source Routing (DSR) performs well in static and low-mobility environments with the routing overhead being proportional to the path length. For secure routing functionality in the network layer, the proposed SCOTRES scheme is integrated with the DSR.

Categorizing a node as trusted, legitimate, selfish or malicious is performed after evaluating a new transaction for this specific node. The evaluation of a transaction’s result is the main function of the protocol that assesses direct and indirect knowledge based on the SCOTRES’s metrics. Indirect recommendations can then be sent to trusted and legitimate 1-hop neighbors, whenever the status of an inspected node changes. The paths that contain malicious nodes are excluded, thus, the malicious activity is addressed and several attacks are countered. Fig. 1 depicts the evaluation process and the underlying parameters of the five metrics that are described in the subsections below.

A. Network Assumptions

This paper concentrates on wireless sensor networks and wireless ad-hoc networks with no or low mobility. Consider an ad hoc network with nodes \( N = \{1, 2, \ldots, i, \ldots, k\} \). We assume that all links are bidirectional. If node \( i \) can receive packets that are directly transmitted by node \( j \), then node \( j \) can
receive packets that are directly transmitted by node \(i\). The wireless network is modeled by a directed graph \(G = (N \cup \{d\}, L)\), where \(d\) is the destination or sink, \(L \subseteq \{(k_1, k_2): k_1, k_2 \in N \cup \{d\}, k_1 \neq k_2\}\) represents the set of communication links.

Attacks on routing and forwarding are mainly studied. We assume that there exists a secure underlying mechanism that is performed by all nodes and accomplishes authentication and confidentiality network-wide. Studies that apply broadcast authentication protocols [26], [27] or lightweight authenticated encryption [13], [29] can be embodied. They provide required security properties, like authentication, integrity check, and resistance to replay attacks, thus, safeguarding forwarding packet misuse. These mechanisms also counter the identity-based attacks (i.e., impersonation, clone ID, Sybil or newcomer attacks, injecting arbitrary packets, and HELLO flooding).

### B. Topology Metric

Topology-based attacks are critical in WSNs and ad-hoc networks. Moreover, they are more effective in settings with trusted components. Malicious entities take into consideration the network’s topology in order to manipulate, disclose or prevent access to legitimate components of high importance and cause more damage.

Nevertheless, relevant countermeasures are not well studied. SCOTRES analyzes the routing table data to discover the topological features of the network. It specifies the topological significance of each evaluating node based on the information that can be mined by the routing information that each node already possesses. Thus, nodes that are significant for the network topology are considered more important for the system’s durability. For these nodes, the rating system becomes more tolerant in cases of failure and, thus, it is harder to classify them as malicious, countering a high variety of topology-based attacks.

The topology metric is calculated by every node. It determines the importance of each related node for the own routing operation. The first parameter of the topology metric is the ratio of paths that a node participates in, called Path Participation (PP). Nodes with high participation are important, as they serve the packets of many paths. The rating component becomes tolerant in cases of failure and the path-selection component balances the communication effort through alternative paths (contributing to the overall load-balancing). The parameter reveals the paths that must be re-established in case that the evaluating node is falsely recognized as malicious (which decreases performance).

However, a malicious node could also participate in many paths to gain high topological significance. Still, the reputation component will force it to serve the high communication effort from all these paths in order to avoid being expelled. Tolerance thresholds are estimated in order to retain the reputation of legitimate nodes in cases of topology-based attacks (preventing the attack), while punishing or forcing to cooperate nodes that try to exploit the metric.

The second parameter of the metric is the ratio of destinations that are uniquely reachable through an examined node, called Unique Path Participation (UPP). Expelling a node as malicious will also derive these destinations unreachable. The rating component is tolerant to such nodes in order to prevent false accusations in case of attacks and punishes a malicious node that exploits the metric after passing a relevant tolerance threshold.

Based on PP and UPP, the topological significance parameters are estimated and utilized in the reasoning process of SCOTRES. The Node Topological Significance (NTS) is the weighted summation of the node’s PP and UPP parameters.

In the routing operation, a path from a source to a destination needs to be selected. The Path Topological Significance (PTS) is calculated as the average NTS value for all path’s nodes. The topology metric is a lightweight feature with low computation overhead, as the four parameters are only calculated whenever routing changes occur.

### C. Energy Metric

Energy consumption is crucial for the examined applications, like green networks. The routing operation should balance the communication effort among the nodes in order to retain their longevity.

Many routing protocols base the selection of the more suitable route on the shortest path, without considering the remaining energy of the selected nodes. Similarly, many trust and reputation schemes select the short paths with well-reputed nodes (e.g. [9], [10]). However, as legitimate nodes consume their resources to serve others, they will continue to be selected as the most appropriate forwarding nodes. If they try to avoid the additional effort and save resources, their reputation is harmed.

To address the above issue, routing protocols are designed that integrate the energy consumption data in the path selection process [11]. The nodes exchange their remaining energy level. Such systems are considered efficient when applied on legitimate networks as they achieve good load-balancing, but they are still vulnerable to attacks [17], [18]. Selfish nodes report low levels of remaining energy to avoid selection, while malicious nodes report high levels of energy to inform their participation. Moreover, attackers identify nodes with low energy (which may be more vulnerable to attacks) or exploit the energy information exchange mechanism to attack the network.

In a typical wireless routing protocol, the nodes operate in promiscuous mode in order to overhear the communication channel and update their routing data. For the energy metric, this mechanism is also considered, in order to enrich the information that is mined by the overheard communication and make decisions about the energy consumption of the evaluating nodes based on self-observation and not on exchanging knowledge. Although the exact energy level is not specified, the extracted information is adequate for achieving efficient energy and load-balancing.

This backpressure algorithm chooses the least busy nodes to forward packets. Combined with the rest metrics, it enhances both performance and security. Every node that overhears the
communication channel, records the participation of the rest nodes. Specifically, they register the number of packets that have been forwarded in a time-window. A node that participates as intermediate in many transactions in the current time-window, has consumed a corresponding amount of energy. This is the first parameter of the energy metric, called the Forwarding Effort (FE). The nodes that have consumed excessive energy (an amount beyond a threshold), are given the excess-energy-consumption bonus.

The second and the third parameters of the metric act as a defense mechanism against selfish and malicious attacks that aim to overload the network. Except from measuring the participation of the intermediate nodes (FE parameter) the energy metric measures the transactions that are initiated by the source and destination nodes. Particularly, the number of packets that the two nodes exchange are noticed down in order to calculate the communication load that they add to the network, forming the Cooperation Load (CL) parameter. If the added load prevents the legitimate node from turning on sleep mode, the relevant CL contribution will be doubled (to limit sleep deprivation). The Fair Cooperation (FC) parameter is the ratio of FE and CL, and reveals the fair usage of the network or its exploitation. A value lower than 1 for the FC, indicates that the node has overburdened the network. After this point, the node is charged regressively. Every additional routing packet through nodes with the excess-energy-consumption bonus counts as two CL ranks. When the FC exceeds a threshold, it discloses a selfish behavior. If a node is categorized as selfish, it is punished and the rest nodes stop forwarding its traffic. Thus, the selfish node is forced to cooperate in order to restore its reputation and later transmit own traffic. When evaluating the energy metric for a path, the average FC values from all path’s nodes are calculated by the Path Fair Cooperation (PFC) parameter. This type of information is utilized by the routing operation.

SCOTRES exploits this information in order to implement an effective energy and load-balancing mechanism, and retain the longevity of the legitimate nodes. For selecting a path from a source to a destination, the system calculates the average node energy consumption of each candidate path. The paths with the lower participation are foregone for serving the new transaction. Moreover, for the nodes that have earned the excess-energy-consumption bonus in the current time-window, the rating component is tolerant to failures and beneficial to continued successful cooperation.

The energy metric maximizes the performance and durability of the network. The legitimate nodes are not excessively burdened and are better safeguarded against attacks that exploit energy consumption. Moreover, the system performs well and is more robust against relevant attacks in congested periods. The computational overhead of the metric is low and, in any case, lower than in the cases of exchanging energy information.

D. Channel-Health Metric

The state of the wireless channel can be affected by several factors; e.g. bad weather conditions and jamming attacks can disrupt the wireless communications. In the case of trust routing schemes, bad channel state causes the failure of several transactions. The trust of legitimate nodes is decreased until they are eventually expelled. The current systems deal indirectly with this occasional malfunctioning by performing automatic reintegration strategies, like periodic re-entrance and redemption [8]. However, malicious nodes are also rejoining to the network.

In [30], an efficient model is proposed to detect and classify jamming attacks in wireless networks. In contract to relevant models [16], it utilizes features that are general and independent from the communication protocol and can be easily implemented by a high variety of WSNs. Specifically, the features of packet delivery ratio, signal strength, and pulse width are deployed to detect constant, random, deceptive, reactive, and short noise-based intelligent jammers. Moreover, the reported results and thresholds for detecting jamming are experimentally validated under real use-cases and attacks.

SCOTRES’s channel-health metric integrates these features. We adopt the aforementioned detection model and implement a jamming-aware routing functionality. In the examined setting, it is only needed to discriminate the normal state of the communication channel from the bad, thus, the whole model is not integrated. Still, it could be fully deployed to provide a more robust intrusion detection mechanism.

For the channel-health metric, SCOTRES utilizes three parameters, which are detailed below. The Packet Delivery Ratio (PDR) is the average successfully received packets and measures the performance of the communication link between two nodes. The receiver measures the packets that have been successfully received (e.g. by checking the Cyclic Redundancy Check, CRC). According to the detection model, PDR is around 78% under normal network operation.

Similarly, at the transmitter side, the Packet Sent Ratio (PSR) measures the average volume of acknowledgements that have been received to the total number of packets that was sent. We consider that the parameter should behave like PDR in normal network operation.

The Signal Strength (SS) measures the power of the signal in dB that is observed at the receiver end. The SS feature is the average signal strength in a time window. When the SS is high, the PDR and PSR are also high, while the converse is not true. At initialization, each node calculates the SS value for every 1-hop neighbor. This value reflects to the ordinary signal strength between two nodes at the normal state. The Signal Strength Variation (∆S) is the change of SS among the ordinary SS value and the SS that it is currently observed.

When the PDR and the PSR go below the thresholds for normal network state (78%), they are collated to the ∆S. If the ∆S is in the boundaries of normal network state, then the glitch is caused by the network. Otherwise, the malfunctioning is caused by the bad channel state (detailed information about the detection of the jamming attack are available in [30]). The Channel-Health (CH) parameter of the metric describes the channel state. ‘1’ is assigned for normal state and ‘0’ for bad channel state after detecting an attack.

In contrast to the original study that only uses PDR, this
work considers both PDR and PSR in order to trigger the health metric either as receivers or transmitters respectively. Thus, selfish or malicious nodes cannot exploit the metric by acting like they are under an attack while successfully transmitting their own traffic at the same time.

When a node detects a bad channel state with one of its 1-hop neighbors in a time-window, it starts becoming tolerant to failures. Moreover, it tries to forward the communication through alternative paths. The path that contains such a 1-hop neighbor gains the bad-channel-health bonus which is subtracted by the path’s overall score in the routing operation. This makes the selection of the path for new forwarding transactions difficult. Thus, the reputation of the legitimate nodes that are under an attack is protected and the performance of the network is retained (both by forwarding the traffic though non-affected routes and by not falsely accusing legitimate nodes as malicious). Thereafter, the system periodically checks the AS parameter in order to detect when the attack is over and restore the affected node’s status.

After detecting a jamming attack, the current solutions, like spread spectrum and frequency hopping aren’t always applicable. Our metric implements a build-in routing protection mechanism that retains the reputation of the legitimate nodes and routes the communication through non-affected paths. We choose this generic strategy instead of the well-known solutions, as it is generic and technology independent, covering a high variety of WSN settings.

The metric requires more resources than an automatic re-entrance strategy. However, the overall robust reasoning process of SCOTRES makes the false accusations of legitimate nodes harder even in bad channel states, making such attack strategies inoperative. Moreover, re-entrance can be more beneficial for attackers than for legitimate entities.

The channel-health metric requires a training session at the initialization phase to determine the normal network state. It then performs simple and lightweight operations with low computational overhead. PDR and PSR are already observed by the reputation schemes. The overall performance of the metric can be considered efficient, as it is an additional security mechanism for a series of problematic cases that are entirely countered by this component.

### E. The Core Reputation and Trust Scheme

SCOTRES applies the state-of-the-art features for the core reputation and trust metrics. The selection is based on a comparative analysis that the authors carried out in [31]. In that study, several trust schemes for secure routing were compared under identical attack scenarios. The internal components and the main reputation and trust features were further analyzed in terms of security and performance.

Reputation evaluates the performance of a node on a specific operation. A reputation structure is implemented for every evaluated operation. This structure maintains all the available information for implementing the reputation features of the specific operation. SCOTRES evaluates the three main operations of routing, forwarding, and making suggestions about other participants – referred to as $R_1$, $R_2$ and $R_3$ respectively. The three reputation structures are identical and implement the reputation features that are described below.

When an operation is performed, a relevant evaluation process is executed to derive the transaction’s result. The outcome is a numeric value that is aggregated in the operation’s reputation estimation for the affected nodes. Initially, it is assigned $+1$ for success and $-4$ for failure (based on the previous analysis in [31]). Then, the three proposed metrics of topology and energy are utilized in order to refine this value and calculate the final outcome for the transaction. The initial rating is multiplied with the NTS, FE and CH parameters. Each of the three parameters is multiplied with a weight, indicating its effect in the final value. The resulting value is aggregated to the relevant reputation structure ($R_1$, $R_2$ and $R_3$) for the examined operation. For routing, SCOTRES evaluates the nodes participation in a route request (i.e. accept or deny) and the validity of the routing information that it broadcasts (e.g. inactive links or loops, and false route breaks) as all messages are authenticated by the underlying cryptographic mechanisms. For forwarding, the system evaluates the forwarding effort that a node serves or evokes and the packet misuse (based on the proper operation of the cryptographic mechanisms). For recommendation, the node is ranked based on the suggestions that is makes for the rest participants, as described in the following paragraphs.

Reputation fading is a core protection mechanism in reputation systems for countering several types of attacks, where a malicious entity gains high reputation in order to be categorized as legitimate and later perform more effective attacks (e.g. Sybil attacks). Fading based on beta or Bayesian distributions is considered more suitable for reputation systems (e.g. [8], [10]). SCOTRES implements a reputation fading mechanism based on the beta distribution. It maintains a history-record of the latest transactions (1000 results, in specific). The operation’s reputation is the weighted summation of these values, with the most recent ones having higher weight. Thus, a reputation fading mechanism is implemented where the latest outcomes are considered more important in estimating the current behavior for a node.

Periodic malfunctioning is a common occurrence in WSNs. SCOTRES enhances the reputation evaluation process by adopting a statistical normalization procedure prior to beta distribution calculation. The historical values are normalized, based on the statistical normalization approach proposed in [31], and then the reputation value is calculated based on beta distribution. This normalized beta distribution system enhances the individual reasoning process of a node that applies SCOTRES; a novel approach in secure routing.

Trust aggregates reputation values from all the evaluated operations and is calculated as their weighted summation. A trust structure for a node contains its three reputation structures. SCOTRES assigns a weight of 20% for the routing, 60% for the forwarding (as forwarding is consider more important for the network durability e.g. [8], [11], [12]), and 20% for the recommending operation (based on a previous security and performance analysis on trust systems for secure routing, conducted by the authors [31]).
SCOTRES is mostly based on direct observation but can also utilize indirect knowledge. There are two evaluation processes for evaluating direct transactions with other participants and for aggregating recommendations made by 1-hop neighbors respectively. Thus, there are two relevant trust structures for each evaluated node. The Direct Trust (DT) structure contains the reputation structures R1, R2 and R3 that are maintained from direct interaction with the evaluated node.

The Indirect Trust (IT) structure contains the DT values that are received from other nodes acting as recommenders. A node only receives indirect knowledge by its legitimate and trusted 1-hop neighbors. For evaluating indirect trust, the deviation test and the weighted summation approaches are combined for ranking the recommenders and aggregating the recommending trust values respectively, as described below.

A deviation test is performed prior aggregating a new recommendation. If the recommendation deviates significantly (namely, more than 30%) from the direct opinion that it is possessed about the evaluated node, the recommender is ranked negatively (as a failed transaction for its direct R) and its recommendation is discarded.

The IT value of a node is the average weighted summation of the recommending DTs. The weight ($W_{ni}$) of each DT is determined by the trust value of the relevant recommender. Thus, the recommendations that are made by trusted nodes gain higher weight.

As in most of the pertinent systems and a previous security analysis (e.g., [8],[31]) a node is categorized as trusted, legitimate, selfish or malicious based mostly on direct observation. Thus, direct knowledge gains higher weight (i.e. 80%) in the total calculation of trust. Based on the three distinct reputations and this aggregated total trust value, thresholds are set for categorizing a node in one of the four aforementioned types (trusted, legitimate, selfish and malicious). Then, the node can make recommendations. As in AODV-REX, the recommender’s privacy is protected by sending this aggregated direct and indirect knowledge.

IV. THEORETICAL SECURITY ANALYSIS OF SCOTRES

In this section, we provide the theoretical analysis of our proposal and its effectiveness in countering the attacker models that are detailed in the simulation study (based on the relevant analyses in [21] and [26] respectively).

A. Theoretical Analysis

Theorem 1 is the main building block of the theoretical security analysis and describes the bounded number of packet loss. At first, we give some definitions and then the theorem and the proof.

**Definition 1:** Let $pkt^+$ be the total number of successfully transmitted packets.

**Definition 2:** Let $pkt^-$ be the total number of lost packets.

**Definition 3:** Let $T_{pkt}$ be the total number of transmitted packets, determined as the summation of $pkt^+$ and $pkt^-$. 

**Definition 4:** Let $\rho$ be the transmission success rate of the totally transmitted packets $T_{pkt}$.

**Theorem 1:** The ideal network exhibits $pkt^- - \rho \cdot pkt^+ \leq 0$. For up to an additive constant, ignoring a bounded number $\varphi$ of packets lost, it holds that the number of lost packets is a $\rho$-fraction of the number of transmitted packets. Specifically, there exists an upper bound $\varphi$, as described in Equation (1).

$$\frac{pkt^-}{\beta} - \frac{\rho \cdot pkt^+}{\beta} \leq \varphi$$

**Proof:** Assume that there are $N$ nodes, $m$ of which are malicious and $m < N$. Let $ML$ be the set of links that are controlled by the malicious nodes. The maximum value of $ML$ is $mN$.

Consider a faulty link $e$, which is convicted $c_e$ times and rehabilitated $r_e$ times. The links weight $w_e$ is at most $mlen$, where $mlen$ is the upper bound of the length of a non-faulty path in the network. If the link’s weight reaches $mlen$ it is considered less efficient that any possible non-faulty path. Therefore, $w_e$ is given by Equation (2).

$$w_e = 2e^{-r_e}$$

Let $\beta$ be the number of lost packets that exposes a path as faulty. The number of convictions is at least $\frac{pkt^-}{\beta}$. Thus,

$$\sum_{e\in ML} c_e < 0$$

Similarly, the number of rehabilitation operations is at most $\frac{pkt^+}{\beta}$. Thus,

$$\sum_{e\in ML} r_e \cdot \frac{pkt^+}{\beta} < 0$$

Therefore,

$$\frac{pkt^-}{\beta} - \frac{ pkt^+}{\beta} \leq \sum_{e\in ML} (c_e - r_e)$$

From Eq. 3, it holds that $c_e - r_e \leq \log w_e$. Thus,

$$\sum_{e\in ML} (c_e - r_e) = \sum_{e\in ML} \log w_e$$

By combining Equation (5) and Equation (6), we derive:

$$\frac{ pkt^-}{\beta} - \rho \cdot \frac{ pkt^+}{\beta} \leq \sum_{e\in ML} \log w_e \leq \beta \cdot mlen \cdot \log mlen$$

Since $\beta = b \cdot \log mlen$, where $\beta$ is the number of lost packets per window, Equation (5) becomes:

$$\frac{ pkt^-}{\beta} - \rho \cdot \frac{ pkt^+}{\beta} \leq \beta \cdot mlen \cdot \log^2 mlen$$

Therefore, the amount of disruption a dynamic attacker can cause to the network is bounded. If there are no malicious nodes Equation (8) describes the ideal case, where $\frac{pkt^-}{\rho} - \rho \cdot pkt^+ \leq 0$.

In contrast with the simple grading that is applied by the most relevant trust schemes and rates failure with -1, gradual grading that is proposed by SCOTRES rates failed transactions with -4.

**Lemma 1:** The gradual grading of SCOTRES decreases the attack rate to at least $\frac{1}{4}$.

**Proof:** Based on Equation (8), it is derived that $4 \cdot b_e \geq b_g$, where $b_e$ and $b_g$ are the number of lost packets per window with simple and gradual grading respectively.

Statistical normalization erase the effects of occasional malfunctioning. Then, reputation fading assigns higher weight
to more recent behavior. Thus, $b$ is further decreased in the current time window due to failures.

The overall load balancing mechanisms of the topology and energy metrics decrease failures in congested periods ($pkt^-$) while enhancing the successful transactions ($pkt^+$). In case of a jamming attack, gradual grading and reputation fading, constrain the number of packet loss ($pkt^-$) until the channel-health metric detects and re-routes traffic, enhancing $pkt^+$.

Selecting the shortest of the most reputable paths instead of selecting the shortest ones, may increase $mlen$, bounding the attacker’s disruption.

When evaluating the forwarding operation, these mechanisms protect the network against ballot-staffing attacks, like blackhole, grayhole, selective forwarding, sleep deprivation and flood rushing. For the routing operation, SCOTRES can detect Hello flooding, routing table poisoning, and false route error. The indirect trust evaluation restricts badmouthing and ballot-stuffing attacks to at most 20%, preventing the establishment of wormholes and sinkholes.

As attacking nodes exceed the malicious threshold they are detected and excluded ($pkt^–\geq m\lambda_{(thr)} \rightarrow (m = m – 1)$). The attack rate is further decreased as $mN$ is decreased. If all attackers are detected $mN$ becomes 0, resulting the ideal case.

B. Attacker Model

We consider active attackers that perform any type of the aforementioned attacks on routing protocols and trust systems. We define the attacker model (Definitions 5-9) and the attack effort (Lemmas 2 and 3), based on the formal analysis of the Ariadne secure routing scheme [26].

Definition 5: Attacker-m-N denotes an attacker who owns $m$ malicious nodes out of the total $N$ nodes of the WSN.

Definition 6: Legitimate-n-N are the remaining $n$ legitimate nodes out of $N$ (where $m+n=N$).

As the volume of $m$ increases, there may be malicious nodes that don’t require to actively participate in the attack.

Definition 7: Active-x-m reports that $x$ malicious nodes out of $m$ were active during the attack.

Definition 8: Counter-y-x refers that $y$ active malicious nodes out of $x$ where successfully countered by the underlying system.

Definition 9: FalseAccused-z-n reveals that $z$ legitimate nodes out of $n$ where falsely countered as malicious nodes.

Lemma 2 and Lemma 3 describe the situation where an attack is considered successful and the attacker’s effort to launch the attack respectively. No proofs are required.

Lemma 2: An attack is successful if either there is one or more malicious node that have not been countered ($|\text{Active-x-m} - \text{Counter-y-x}| > 0$) or there is at least one falsely accused legitimate node ($\text{FalseAccused-z-n} > 0$).

Lemma 3: The effort to accomplish the attack is the percentage of malicious nodes that are required to exploit the system ($\text{mx100}/N$).

Definition 10 determines the attacker’s effectiveness that is utilized in the simulation analysis to assess the SCOTRES’s resilience to different types of attacks.

Definition 10: The effectiveness of a successful attack is designated by the analogy of the malicious nodes that are deployed to the non-countered and falsely accused nodes. Equation (9), defines the attack’s effectiveness ($AE$).

$$AE = \frac{\text{[Active-x-m] - [Counter-y-x]} + \text{FalseAccused-z-n}}{\text{Legitimate-n-N}} \times 100 \% \quad (9)$$

We regard that a system counters an attack if $AE$ is lower than 0.2 and partially counters it if $AE$ is from 0.2 to 0.3. We consider settings where the attacker owns up to 50% of the total nodes. WSNs with higher malicious ratio should be discarded.

V. SIMULATION AND ANALYSIS

NS2 implements the DSR protocol in C++. This implementation is extended to deploy the integrated SCOTRES_DSR. The assignment of all constant coefficients is based on a previous security and performance analysis, conducted by the authors [31] under the same platform. The simulation study revealed the effectiveness of the core components for different reputation and trust settings. Results from relevant studies regarding the thresholds for detecting active attackers [32], [33] are also considered. All these results are adopted by SCOTRES (e.g. the positive and negative reputation rating values). The systems S-D RepIDS, AODV-REX, RFSN, TRDSA, EFW, and SR3 are also implemented on the same platform, in order to provide a fair comparative analysis under the same attack scenarios.

In order to evaluate the various routing mechanisms, a WSN was modeled, consisted of 50 nodes. The two-ray ground reflection model is used for propagation and the IEEE 802.11 Distributed Coordination Function (DCF) is used for the MAC layer. Every node has a raw bandwidth of 2Mbps and a physical radio range of 100m. The simulation area occupies 350m x 350m. Each experiment includes two phases. At initialization, nodes start with the default trust values as defined by each scheme. At evaluation, the normal operation is monitored, as well as four attack scenarios, measuring performance and security. In both phases, 10 source nodes on one end of the WSN send 1KB data with Constant Bit Rate (CBR) to 10 destination nodes at the other end of the WSN. Each phase lasts 1 min.

The first scenario examined was the one of normal operation, i.e. with no attacks taking place. Thus, we compared the normal behavior of the pure DSR and the seven secure routing schemes. One experiment per system is performed, as the result is deterministic for each setup.

Then, malicious nodes are introduced in the WSN in order to perform four types of attacks, determining the security level of the examined systems. For each attack, 5 experiments were performed per system, using 10, 20, 30, 40 and 50 percent of malicious nodes respectively. Each experiment was executed 10 times and the average metrics were calculated. In total, there were 50 iterations for each system per attack. At each iteration, the malicious nodes were assigned randomly. For the first evaluated system, the malicious nodes of each iteration were recorded – a necessary step in order to use the exact
same setting in all systems, ensuring they are compared under identical situations.

A. Normal WSN State

The systems are initialized in the first phase and the following four metrics for load-balancing and power consumption are evaluated.

$M_{1-1}$ is the percentage of inactive intermediate nodes that do not participate in the forwarding operation. A high percentage of inactive intermediates reveals poor load-balancing as a few intermediate nodes serve all the communication effort. $M_{1-2}$ is the average amount of data (in KB) that is forwarded by the active intermediate nodes. The lower the value, the better. $M_{1-3}$ estimates the power consumption by calculating the operations that are performed by each node. One operation unit is added for each reception or sending operation. Based on $M_{1-3}$, $M_{1-4}$ measures the variation of node consumed power (COV). Equation (10), describes the COV metric.

$$COV = \sigma(M_{1-1})/\mu(M_{1-1})$$  (10)

Where $\sigma$ is the standard deviation and $\mu$ is the mean deviation. Energy-balancing is achieved for low COV values. The metrics $M_{1-2}$ and $M_{1-4}$ are utilized to identify the systems that achieve good load- and energy-balancing. The lower the values of the two metrics, the better. Fig. 2, illustrates the evaluation results.

In four secure routing systems (S-D RepIDS, AODV-REX, RFSN, EFW), more than half of the intermediate nodes remained inactive during the experiment and did not forward any packets. This is the result of the typical reasoning process used in such systems. All nodes start with the default reputation values. As the first nodes start forwarding traffic, their reputation is increased and they are continually selected (as no malfunctioning occurs). Thus, a few nodes serve all the traffic. Pure DSR achieve a slightly better load-balancing as it selects the shortest path from a source to a destination. Thus, nodes that are located at the boundaries of the WSN were also selected for some transactions, while in the former case the intermediate nodes at the center of the WSN gain higher reputation and were preferred. TRDSA takes into account the energy consumption. It achieves low inactive-node ratio and forwarding effort. SR3 produce the best dispersion as it entails longer and random routes. This results in higher forwarding effort, as the intermediate nodes participate in more routes than in the rest systems. SCOTRES achieved the best load-balancing performance with the lower average forwarding activity and only 10% of the intermediate nodes remaining inactive.

The load-balancing capability proportionately affects the power consumption and the longevity of the nodes. Thus, SCOTRES consumed the least mean power among the evaluated systems. For the rest of the systems, high values of the COV metric ($M_{1-4}$) reveal that a few active intermediate nodes were overburdened.

B. Attack Scenarios

Four attack scenarios are modelled to evaluate the security of each setting. The attacks target both the trust schemes and the routing protocol vulnerabilities. In the first case, the malicious nodes perform a social-based on-off attack at initialization and a blackhole attack at the evaluation phase. In the second scenario, the attackers perform ballot-based attacks (ballot-stuffing and badmouthing) at initialization, enabling link-spoofing attacks during the evaluation phase. In the third attack, the malicious nodes take advantage of the congested periods and network’s topology in order to make legitimate nodes unavailable through flooding attacks (in forwarding or routing) at the evaluation phase. The goal is to overburden these legitimate nodes and make them misbehave, harming their reputation. In the last attack, the malicious nodes perform constant jamming attacks at the evaluation phase. The affected nodes start misbehaving as they cannot properly send and receive data and their reputation is decreased.

Under a blackhole and jamming attacks, the performance of...
a system is measured as the delivery ratio – the percentage of the packets that were successfully transmitted from the source to the destination to the total packets that were sent, defined as $M_2$ and $M_3$ respectively. The higher the value, the better. The link-spoofing effect, metric $M_4$, is calculated as the percentage of the total transactions that were routed through paths that contain at least one malicious node due to the effect of the ballot-based attacks. The lower the value, the better. The metric $M_4$ calculates the number of legitimate nodes that were rendered unreachable by the energy- and topology-based attacks. The lower the value, the better. Fig. 3, illustrates the resulting metrics.

The evaluation of DSR reveals the effectiveness of the attack on an unprotected system. The systems’ performance worsens as the malicious nodes increase. In general, systems that can quickly discover the malicious nodes achieve high detection ratio and retain network’s performance by eliminating the negative effects. As the malicious nodes increase, the delivery ratio is decreased, while the average affected transactions per source node are increased. The detection ratio follows a conflicting behavior. As the volume of the malicious nodes increases, many malicious nodes participate in the same path. Thus, the first malicious nodes perform the attack until they are detected and punished, while the rest of the malicious nodes could remain inactive during the evaluation phase.

TRDSA and EFW perform poorly under blackhole attacks due to their simple transaction evaluation processes and slow adaptability. SR3 detects malfunctioning faster, but the lack of recommendations and the high dispersion lead each one of the source nodes to come across almost every malicious node. AODV-REX, RFSN, S-D RepIDS and SCOTRES discover the attackers faster, due to the reputation fading feature. SCOTRES achieves the best results due to the more robust reasoning process for evaluating direct knowledge and making recommendations.

Badmouthing attacks lower the trust level of legitimate nodes and harden their selection as forwarding nodes. As a result, the malicious nodes with legitimate trust are preferred and their trust is increased. Similarly, ballot-stuffing increases the trust values of malicious nodes. Then, malicious nodes are preferred for forwarding while legitimate nodes participate in less transactions and their trust level is decreased. In all cases, as the malicious nodes increase, their average trust value is also increased, while the average trust value of the legitimate nodes is decreased. Thus, the link-spoofing succeeds in both cases.

The ballot-based attacks that are performed are determined by the type of recommendations that are imposed by the evaluated system. S-D RepIDS and TRDSA use negative recommendations (badmouthing). RFSN and SCOTRES utilize both negative and positive recommendations (both badmouthing and ballot-stuffing). SR3 are based on acknowledgement messages to verify a successful transmission. In that cases, the colluding attackers drop the acknowledgement in paths where the legitimate nodes are more than 50%. Thus, a high rate of legitimate nodes can be falsely accused, while paths with many malicious nodes are seem reliable. The pure DSR and EFW are not evaluated in this scenario, as no recommendations are used.

SR3 is vulnerable to acknowledgement misuse and produces the highest false accusations and link-spoofing effect. TRDSA also achieves high false accusation ratio due to badmouthing as it does not properly handle negative recommendations; the system accepts these when they originate from trusted nodes or from malicious leaders with higher trust respectively. Thus, malicious nodes who cooperate in the initialization phase, exploit the recommendation operation. S-D RepIDS is less vulnerable to badmouthing as it gives higher weight in direct knowledge (a node is recognized as malicious only by direct interaction). AODV-REX, RFSN and SCOTRES deal with both attacks as the recommendations are also collated with direct knowledge.

With regard to link-spoofing, SR3 provides little protection. TRDSA uses simple recommendation operations that cannot effectively counter such an attack. AODV-REX weights direct and indirect knowledge the same; making it vulnerable to high ratio of attackers. S-D RepIDS uses more advanced mechanisms for mitigating these effects. RFSN is the best among the examined systems of the related work. SCOTRES implements an even more robust recommendation evaluation mechanism and rates the recommenders against direct interaction. It is the only evaluated system that can detect the ballot-stuffing attacks and successfully counter the link-spoofing effect. For $M_3$, SCOTRES achieves the best result as it stops the link-spoofing attack, once the bad recommenders are detected and punished.

The nodes that were found vulnerable due to congested periods were mostly located at the center of the WSN, where the bulk of the data was forwarded to. The nodes that were vulnerable to topology-based attacks were located at the boundaries of the network, connecting source or destination nodes with the rest network. From the evaluated systems, DSR, AODV-REX, RFSN and EFW provide no special treatment for congested periods or topology-based attacks. S-D RepIDS provides protection in congested periods. SR3 reduces congestion traffic due to the random nature of the random walk algorithm. TRDSA makes energy-aware decisions about routing and mitigates the energy-based attacks. SCOTRES protects the network in both cases.

The most flooding attacks were performed under DSR, AODV-REX, RFSN and EFW. For DSR, there were some paths that were rendered unavailable and falsely considered as broken. AODV-REX and RFSN perform the same and exhibit the most false accusations and unreachable nodes. S-D RepIDS exploits its fault-tolerance mechanism in congested periods, mitigating the false accusations. The MAC-layer measurements of EFW assigns low communication reliability to the overloaded links. It routes the traffic through alternative links mitigating the false accusations. In the cases of TRDSA, SR3 and SCOTRES, mostly topology-based attacks were performed, as the load-balancing mechanisms mitigated the overloaded nodes and the relevant flooding attacks. SCOTRES detects the flooding as malicious activity when it is
performed in congested periods through overload nodes or topological-significant nodes. It demonstrated the best behavior in terms of countering the attack, as there was only one false accusation in the scenario involving 50% of malicious nodes, and all source and destination nodes remained reachable.

For a high volume of jamming attackers (50%) no communication could be accomplished, as they disrupt all the paths from the source nodes to the destinations. DSR and the five secure routing schemes (S-D RepIDS, AODV-REX, RFSN, TRDSA, SR3) perform poorly, even under a small number of attackers. EFW and SCOTRES are the only system to implement a fault tolerance mechanism to mitigate the effect of a jamming attack, achieving a good delivery ratio, up to a certain amount of jammers (10% - 30%). SCOTRES is more advanced as the health-metric is responsible for detecting jamming attacks. Moreover, the reputation of the legitimate nodes is protected in any case, as there were no false accusations even with 50% of malicious nodes.

C. SCOTRES’s Measured Resilience

We model as an Attacker-m-50 the nodes that perform the aforementioned attacks in the four scenarios. In the first two cases, SCOTRES successfully countered the attacks for all Active-x-m that were evaluated without any false accusation (Active-x-m = Countered-x-x, and FalselyAccused-0-n). The AE was 0 for all models. In the third case, the active malicious nodes were always detected while there was a small number of false accusations for high ratio of malicious nodes. The best attack achieved 1 false accusation (FalselyAccused-1-25) for Attacker-25-50, with AE=0.02. SCOTRES successfully countered all three types of attacks. In the fourth case, all malicious nodes were active (Active-m-m), FalselyAccused-0-n holds in all cases. SCOTRES successfully countered the attack for low ratio of malicious nodes (Attacker-5-50 achieved AE=0.1, Attacker-10-50 achieved AE=0.15). For medium volume of attackers, it partially countered the attack (Attacker-15-50 achieved AE=0.23). Little to no protection was provided for high number of attackers (Attacker-20-50 achieved AE=0.35, Attacker-25-50 achieved AE=0.5).

VI. REAL-WORLD IMPLEMENTATION

In addition to the NS2 simulations, SCOTRES is also deployed on real embedded platforms and mote devices, implementing an agricultural application.

A. Precision agricultural CPS

A precision agricultural CPS is considered, where the devices collect environmental parameters (e.g. temperature and humidity) and transmit them to a processing center (laptop with WiFi capability). The processing center publishes the measurements to a cloud management system (e.g. [34]), where the user can gain access via Internet connection. Then, the farmers make decisions regarding fertilizer application, watering, pruning, digging or other rural activities.

The user can access the aforementioned functionality through cloud. The application is implemented on the Greek Research and Academic Community cloud service, named okeanos [35].

The system is tested in a rural settlement of a small village of the Crete Island in Greece. The WSN monitors two small forests and one olive grove, nearby the village. The devices transmit the measured parameters every one hour, total 24 transmissions for each device per day. The processing center is located at the community’s public building and the users have access through the community’s free WiFi connection that covers the whole village. Fig. 4 illustrates the application setting.

B. Embedded platform

SCOTRES is implemented on real embedded devices and its overhead compared to the pure DSR protocol was measured. The DSR-UU implementation of the routing protocol is extended and deployed on BeagleBone devices (low-cost credit-card-sized embedded device that runs a compact Linux OS). A network of ten BeagleBone devices is created and connected wirelessly via a USB Wi-Fi module.
We measure the overhead that is added to the DSR-UU protocol by the SCOTRES scheme during normal network conditions (i.e., without any attacks) in terms of executable code size (KBs in ROM), and average memory requirements (RAM consumption in bytes) and processing delay (ms of CPU time). Measurements were taken for a one day operation of each system. The three proposed SCOTRES metrics for topology, energy and channel health consume little resources. The reputation calculation is the most resource-consuming component, due to the history of past values that is maintained for each evaluated operation. This feature proportionally affects the resource consumption of the trust metric. The added overhead for routing and forwarding is low. Thus, the average network latency (end-to-end communication) is also low, around 0.5 sec. Fig. 5.A depicts the latency of two randomly selected nodes. The integrated SCOTRES_DSR-UU requires around 50% more memory and 70% more computational resources than pure DSR-UU. The proposed system consumes more resources, however, the additional overhead can be considered acceptable for the combination of good security and load-balancing behavior that it achieves. Fig. 5.B, summarizes the overall resource consumption.

C. Mote devices

As a proof of concept, we also apply SCOTRES on Zolertia Z1 motes. Z1 is a low-power WSN module that runs the Contiki OS. It uses a single core 16-bit RISC CPU at 16 MHz (MSP430F2617 microcontroller) with 8 KB RAM and 92 KB flash memory. Z1 is equipped with build-in temperature (TMP102) and accelerometer (ADXL345) digital sensors. The networking features include the CC2420 transceiver at 2.4GHz, enabling communication with IEEE 802.15.4 and 6LowPAN. A wire antenna is utilized with radio range of around 25 meters. It is powered by two AA batteries (3.3V) or through a u-USB port (5V).

We apply SCOTRES on Z1 motes that are powered by batteries and communicated wirelessly the sensed temperature via IEEE 801.15.4 with 6LowPAN. In order to reduce the resource consumption, the history elements of each reputation structure is reduced from 1000 to 100. Moreover, all data structures and variables are becoming static with fix size to minimize the RAM usage. We measure the power consumption in mW, the energy dissipation (the time instance since the network deployment until the first node exhausts its energy below the minimum energy required for transmission under any channel condition) and the network life time in months of operation (the time duration from the instant of the sensor network deployment to the instant that the signal field cannot be reconstructed with a given QoS requirement from the current live sensors) under a lab setting and the aforementioned rural application.

Under the lab setting, the motes continuously transmit data. On average a mote running SCOTRES consumes 5.87 mW. It takes around 15 days until a mote runs out of energy. Under the rural application setting, the motes run SCOTRES to transmit data and evaluate the result every one hour (not continuously). The energy dissipation is around 40 months and the network life time is 50 months.

VII. CONCLUSIONS

This paper presented SCOTRES – a trust system for secure routing. SCOTRES is implemented in the NS2 simulator and is integrated with the DSR routing protocol. A comparative analysis is also included in this work, involving SCOTRES, DSR and six other secure routing schemes. Five application scenarios are modeled in order to evaluate the security and performance of each system. As is evident from this broad evaluation, SCOTRES demonstrates the best energy- and load-balancing behavior, provides the highest level of security, and deals with some types of attacks that the rest of the systems cannot counter. SCOTRES is also applied on real embedded platforms and mote devices, in the context of a rural CPS that communicates information to the cloud. The overall evaluation also indicates that the overhead of the trust system is relatively low and acceptable for the combination of security and node longevity that it is offers.

REFERENCES

mailholders%20press%20release.pdf


[35] Greek Research and Academic Community, okeanos cloud services. Available online at: https://okeanos.grnet.gr/home/

G. Hatzivasilis is a PhD candidate at the ECE department of the Technical University of Crete, Greece. He received his M.Sc. and B.Sc. in Computer Science from the University of Crete. His research interests include IoT systems, lightweight cryptography, trust management, and ambient intelligence.

Dr. I. Papaefstathiou holds a PhD degree in computer science from the University of Cambridge. He is an Assistant Professor at the ECE Department of the Technical University of Crete. His current research interests focus on architectures for network processors and specific purpose networking systems.

Dr. C. Manifavas holds a PhD in Computer and Communications Security from the University of Cambridge. He is an Associated Professor at the Electrical Engineering & Computing Sciences Department of the Rochester Institute of Technology in Dubai. His areas of interest include information security management, security protocols and cryptography.