Reputation-Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review

Hani Alzaid, Manal Alfaraj, Sebastian Ries, Audun Jøsang, Muneera Albabtain, Alhanof Abuhaimed

▶ **To cite this version:**

Hani Alzaid, Manal Alfaraj, Sebastian Ries, Audun Jøsang, Muneera Albabtain, et al.. Reputation-Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review. 7th Trust Management (TM), Jun 2013, Malaga, Spain. pp.66-82, 10.1007/978-3-642-38323-6_5 . hal-01468184

HAL Id: hal-01468184
https://inria.hal.science/hal-01468184

Submitted on 15 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Reputation-based Trust Systems for Wireless Sensor Networks: A Comprehensive Review

Hani Alzaid[1⋆], Manal Alfaraj[2], Sebastian Ries[3], Audun Jøsang[4], Muneera Albabtain[1], and Alhanof Abuhaimed[1]

[1] Computer Research Institute, King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia
[2] Almaarefa College, Riyadh, Saudi Arabia
[3] CASED, Hochschulstrasse 10, 64293 Darmstadt, Germany
[4] University of Oslo, PO Box 1080 Blindern, 0316 Oslo, Norway

Abstract. Cryptographic mechanisms alone are insufficient to protect Wireless Sensor Networks (WSNs), because sensors are deployed for long periods in hostile environments where it is possible for an adversary to physically take over a sensor and obtain access to the cryptographic keys stored in the sensor's internal memory. Thus, reputation-based trust systems are employed to detect abnormal activities and enhance the trustworthiness among sensors. Unfortunately, existing reputation-based trust systems for WSNs do not investigate the robustness against WSN-related or reputation-related attacks. This paper provides a comprehensive analysis for current reputation-based trust systems by surveying the current "state-of-the-art" work in this area.

Keywords: reputation; sensor networks; taxonomy; ballot; bad mouthing; newcomer; on-off; selective forwarding; sybil; spoofed data; replay

1 Introduction

Wireless Sensor Network (WSN) is a highly distributed network of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or other systems by the measurement of physical parameters such as temperature, pressure, or relative humidity [1, page 647]. Sensor nodes collaborate to form an Ad Hoc network capable of reporting network activities to a data collection sink.

Sensor nodes are typically powered by batteries. Therefore, the energy impact of adding security features should be considered. For example, data authentication in TinyOS increases the consumed energy by almost 3%, while data authentication and encryption increases the energy consumption by 14% [2]. Furthermore, the processing capabilities in sensor nodes are generally not as powerful as those in the nodes of wired networks. Complex cryptographic algorithms are consequently impractical for WSNs.

WSNs are assumed to be deployed in remote or hostile environments where nodes can be exposed to physical attacks. An adversary can easily compromise one or more sensor nodes and extract secrets which could affect the overall performance of the network. This attack is referred to as the node compromise attack [3, 4]. Sensor node compromise is a realistic threat, because the current

⋆ corresponding author, email (hmalzaid@kacst.edu.sa).

sensors are mass-produced devices without tamper-resistance. Even worse, the adversary may also inject their own commodity nodes into the network by fooling nodes into believing that these commodity nodes are legitimate members of the network, especially if there is no proper authentication scheme in place. Another adversary activity is launching Selective Forwarding attack where a node, which is under the control of an adversary, selectively drops legitimate packets in order to affect the overall performance of the system [18]. A simulation study presented in [19] showed that the network operation and maintenance can be easily jeopardized and network performance will severely degrade once a single node starts misbehaving.

This paper introduces a comprehensive analysis of the current reputation-based trust systems and the security attacks they suffer from. It is believed that this comparison is helpful to establish common ground (or test-bed) and distinguish between existing reputation-based trust systems. This will help drawing a road map for the future design of attack resistant reputation-based trust systems for WSNs.

The rest of the paper is organized as follows: Section 2 highlights similar works in literature. Section 3 discusses the security concerns in reputation-based trust systems designed for WSNs. A comprehensive survey of the "state-of-the-art" in reputation-based trust systems for WSNs is accomplished in order to build an analysis framework for reputation systems. The framework is discussed in details in Section 4. Section 5 compares in details these reputation-based trust systems. This comparison includes: investigating the visibility of the main components of the reputation systems, and studying the appearance of attacks, which are related either to WSNs or reputation systems, in existing systems. Finally, the paper is concluded in Section 6.

2 Background

The most cited definition of trust is presented by Dasgupta as "the expectation of one person about the actions of others that affects the first person's choice, when an action must be taken before the actions of others are known" [5]. This definition captures both the purpose of trust and its nature in a form that can be reasoned. Though many definitions are available in the literature, a complete formal unambiguous definition of trust is rare because trust is a complex term with multiple dimensions.

A concept that is often mentioned together with trust is reputation. To avoid confusion, a definition for reputation as well as the relation between reputation and trust are highlighted in this paragraph. Jøsang et al. [6] define reputation as "what is generally said or believed about a person's or thing's character or standing". Although the definition only introduces an abstract notion of reputation, it allows one to easily differentiate between trust and reputation. Trust describes a subjective relation between an entity and another entity (or group of entities) while reputation is what is generally said about an entity. Thus, the reputation of an entity is based on the opinions provided by all entities. Trust may be used to determine the reputation of an entity. The other way around, reputation may also be used to determine the trustworthiness of an entity [6].

The feedback forum on eBay is the most prominent example of online reputation systems [7] in which the basic idea is to let parties rate each other. After the completion of a transaction, each party is allowed to leave feedback about their experience of the other party. Then, the aggregated ratings about a given party are used to derive a reputation score, which can assist other parties in deciding whether or not to deal with that party in the future.

In general, trust and reputation models provide means for assessing the trustworthiness of an entity within a specific context or scope. However, traditional trust management schemes used for wired and wireless Ad Hoc networks are not suitable for WSNs due to higher computational costs, and large memory and communication overheads [10]. There are numerous approaches for trust and reputation models that have been destined to the field of WSNs [11–17]. In WSNs, an entity usually is a sensor node or a cluster head; the entity scope varies from a system to another. For example, the scope can be ensuring whether a node is expected to report its sensor information truthfully or whether it is expected to forward packets reliably. Thus, reputation systems provide means for making WSNs more fault-tolerant and more robust to attacks. Unfortunately, due to the lack of common ground for these systems, they have led to different trust system architectures and different attack-resilient levels.

3 Security Concerns

Integrating reputation system capabilities within WSNs helps strengthen the performance and security levels of WSNs by providing continuous monitoring, and warning neighbors about malicious behaviors. Although the usage of trust and reputation concepts does not prevent attacks, these concepts help detect malicious behaviors and then exclude from the network nodes that caused these malicious behaviors. As we propose to increase the robustness of WSNs by reputation systems, two types of attack may threaten the proposal robustness. These two types are: (i) WSNs-related attacks (WSNs attacks) and (ii) reputation-related attacks (reputation attacks) as discussed in the following subsections.

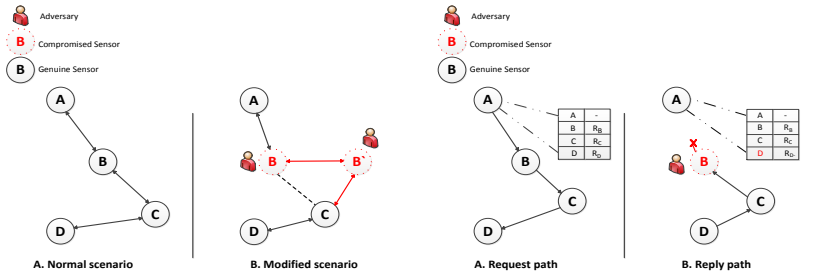
3.1 WSNs Attacks

WSNs are vulnerable to different types of attack due to the nature of the transmission medium (broadcast), remote and hostile deployment location, and the lack of physical security in each node [20]. These attacks are as follows:

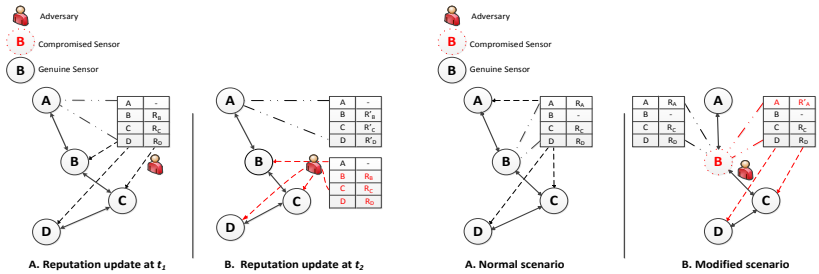
Sybil Attack (SY) A node that wishes to conduct the SY attack[1] can create new multiple identities to affect the reputation values of legitimate nodes in reputation-based applications by falsely degrading their reputation values.

For example, the real path in Figure 1(a)-A starts from node $A(D)$ and ends at node $D(A)$. Nodes B and C are adjacent neighbors. A simple form of the SY attack occurs when the adversary has the ability to compromise some nodes. Suppose that the adversary succeeded in compromising node B and then manipulating the route discovery messages within the routing activities. Thus, the adversary can add another node to the network, which is node $B^{'}$ in Figure 1(a)-B.

[1] It has also been defined as a malicious device illegitimately taking on multiple identities.



(a) Sybil Attack (b) Selective Forwarding Attack



(c) Replay Attack (d) Spoofed Data Attack

Fig. 1. Wireless sensor networks attacks: (a) Sybil Attack, (b) Selective Forwarding Attack, (c) Replay Attack, (d) Spoofed Data Attack .

Now, the adversary can communicate with node A using node B and communicate with node C using node $B^{'}$. The adversary can perform malicious activities in the network and trickily blame node $B^{'}$ (or node B) for those activities and leave the reputation value of node B (or node $B^{'}$) untouched.

Selective Forwarding Attack (SF) It is assumed in WSNs that each node will accurately forward received messages. However, a compromised node may refuse to do so. It is up to the adversary controlling the compromised node, whether to forward received messages or not. Once the adversary has succeeded in launching a SF attack, it can affect the propagation of reputation information such as direct observations across the network. Note that SF attacks are most effective when the attacking nodes are included in the path of the data flow.

The scenario, in Figure 1(b), follows the single aggregator model [21], where node A acts as an aggregator. In Figure 1(b)-A, the adversary succeeded in compromising node B but behaved well and forwarded the request message sent by node A. Later on, node B, which is still under the adversary control, drops the response from D as in Figure 1(b)-B. Subsequently, the aggregator has not received any reply for its recent request. Consequently, node A updates its rep-

utation table and keeps the out-dated reputation value of node D or reduces it due to aging as in Figure 1(b)-B.

Replay Attack (RE) This attack is the easiest one because the adversary does not need to physically capture a node and get access to its internal memory, or analysis encrypted data. The adversary can record some reputation information, which has been exchanged wirelessly between sensor nodes, without even understanding its content and then replay them (with no changes) to mislead other nodes and bring their reputation tables out-dated. Suppose an adversary captured a reputation update message at time t_1 (see Figure 1(c)-A), and then re-injected it at time t_2 where $t_2 > t_1$ (see Figure 1(c)-B). With no proper verification, nodes B, C, and D will accept this re-injection and end up with out-dated and thus potentially incorrect reputation values.

Spoofed Data Attack (SD) This attack cannot be launched alone; the adversary needs to combine either a RE attack or node compromise attack with a SD attack. In the former, the adversary first eavesdrops on the traffic, captures some reputation information in understandable format, performs some changes on the captured information, and then re-injects it into the network. In the latter, the adversary first needs to overtake a node, and can then affect the reputation calculation by falsely claiming that his direct observation for node N_i is $R_i^{'}$ (instead of the correct R_i). $R_i^{'}$ is then propagated to neighboring nodes which are misled by the received indirect observation $R_i^{'}$ and thus their calculations for the reputation value of N_i are affected. For example, the adversary in Figure 1(d)-B, during the reputation update phase, claims that the reputation value for node A is $R_A^{'}$ not R_A and then sends it to the neighboring nodes C and D. Therefore, nodes C and D will use $R_A^{'}$ as an indirect observation for node A when they calculate the reputation value for node A.

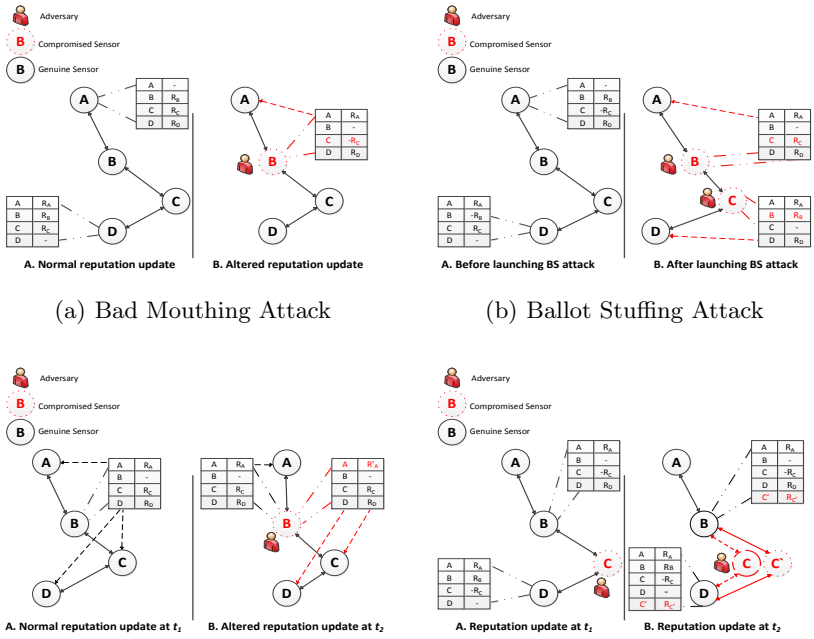
3.2 Reputation Attacks

The reputation system itself is threatened by several types of attacks [22, 23]. Understanding these attacks is crucial to ensure that the integration between reputation systems and WSNs does not open doors for more threats. Attacks that are only applicable to the reputation system are discussed as follows:

Bad Mouthing Attack (BM) This BM[2] attack concerns with providing unfair negative ratings for trustworthy nodes. Once the adversary has compromised a node, it can affect the reputation system by assigning falsely negative feedback as the compromised node's observation of well-behaved neighboring nodes. When these incorrect direct observations are propagated to other nodes, they will be considered by neighboring nodes at the reputation calculation phase if no proper verification is in place, as will be discussed in Section 4. This results in incorrect reputation values for victim "well-behaved" nodes. This attack is visible in scenarios where the indirect observations are considered and parties are allowed to share their negative feedback with nodes in the neighborhood.

Figure 2(a)-A shows the normal reputation update where nodes A and D have the same reputation value R_C for node C. In figure 2(a)-B, the adversary has succeeded in compromising node B. Later on, it assigned a negative reputation

[2] It is also known as False Accusation attacks.



(a) Bad Mouthing Attack (b) Ballot Stuffing Attack

(c) On-Off Attack (d) Newcomer Attack

Fig. 2. Reputation attacks: (a) Bad Mouthing Attack, (b) Ballot Stuffing Attack, (c) On-Off Attack, (d) Newcomer Attack.

value $-R_C$ for a well-behaved node C in order to mislead node A with its calculation of the reputation value of node C. Consequently, nodes A and D have different reputation values $-R_C$ and R_C, respectively.

Ballot Stuffing Attack (BS) A ballot attack is similar to the BM attack, but the adversary tries to perform the opposite effect by providing unfair positive ratings (false praise). The trustworthiness of the bad-behaved nodes is affected by assigning falsely positive feedback to malicious nodes. This attack is visible in scenarios where the indirect observations are taken into consideration and parties are allowed to share their positive feedback with their neighboring nodes. Nodes B and C, in Figure 2(b)-A, are compromised and their reputation values (or maybe one of their reputation value) are low due to their previous malicious behaviors. These compromised nodes colluded with each other and assigned higher reputation values to each other as in Figure 2(b)-B, which will affect the reputation calculation for nodes B and C at nodes A and D.

On-Off Attack (OO) The adversary, in this attack, aims to disturb the system's overall performance with the hope that it will not be detected or excluded from the network. The adversary alternates in showing abnormal and normal

behavior in order to extend the detection time required to recognize its misbehaviors. This attack can be launched against either the reputation activities or general activities in WSNs.

Figure 2(c)-A shows a subset of genuine nodes where a node B shares its reputation table with neighboring nodes. Let us assume that node B has been compromised at t_2 where $t_2 > t_1$. Later on, node B behaves maliciously intermittently when it deals with nodes C and D by claiming that the reputation value for node A is $R_A^{'}$ instead of R_A. However, it behaves normally when it deals with node A and disseminates the real reputation values for nodes C and D (see Figure 2(c)-B). Another form of the OO attack happens when a sensor node misbehaves once every t well-behaved transactions, which makes nodes A, C and D uncertain about the behavior of node B.

Newcomer Attack (NC) As soon as the adversary's reputation value drops below the threshold value, which moves the node from a trusted mode into a distrusted mode, the adversary will consider other ways to increase its reputation value. One way to do so is to rejoin the network with a new ID and wipe out all its bad history. This attack is referred to as the newcomer attack[3]. If the adversary has the ability to launch this attack, then detecting the adversary's misbehaviors is not an issue from the adversary's perspective due to the fact that all the old history can be wiped out at any stage.

A sketch of a simplified scenario for a NC attack is shown in Figure 2(d). The reputation value of node C in Figure 2(d)-A fell below the predefined threshold value as a result of its previous misbehaviors. Thus, the adversary may rejoin the network with a new identity $C^{'}$ and neutral reputation value as in Figure 2(d)-B.

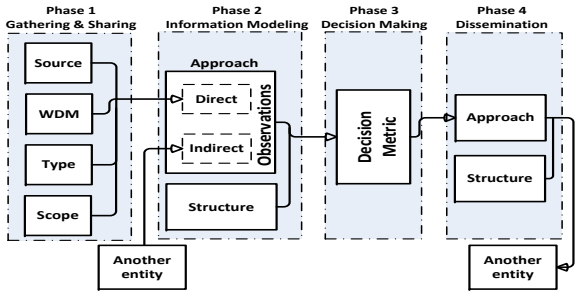


Fig. 3. The reputation system phase s

4 Analysis Framework for Reputation Systems

Reputation systems often share similar structural patterns due to the common purposes they are used for. It is found that they consist of four main phases: information gathering and sharing, information modeling (or reputation calculation), decision making, and dissemination (See Figure 3).

4.1 Information Gathering and Sharing Phase

It compromises the communication and collection of reputation ratings. The system design must specify the type of information to be collected about other

[3] It is sometimes referred to as the identity attack or white washing attack [24].

neighboring nodes, and how it should be collected. The metrics for collected ratings can for example accept only positive ratings, only negative ratings, both types, or any rating on continuous scales. The information gathering and sharing phase is composed of four components as follows:

Information Source: The process of creating information in any reputation system can be either manual or automatic. An example for manual created information is user ratings as a result of being involved in a single transaction such as in the eBay rating system [7]. This type of source is not available in WSNs due to the lack of user interaction with the network. The automatic information resource on the other hand does not involve user interaction and can be either direct or indirect observations. Direct observations, sometimes called first-hand information, are computed based on the node's observations and experience about neighboring nodes. In some reputation systems, the direct observation needs to be propagated to other nodes in the neighborhood and then this propagated information is called indirect observation, or second-hand information, at the receiving nodes. Indirect observation helps building up the reputation system more quickly than using only direct observation since nodes will be able to know about other nodes' behaviors even though no direct communications have occurred. However, propagating reputation information between nodes makes the system vulnerable to attacks as discussed in Section 3.

Information Type: The type of the reputation information shared between sensor nodes can be unary, i.e., either only negative [11], or only positive [25], or binary, i.e., meaning positive or negative [14, 26], discrete, i.e., positive, neutral, negative as in eBay, a natural number on a scale from 1 (untrusted) to 10 (trusted) [9], or continuous [27], e.g., real values in the range of [0,1]. The designers should be aware of the consequences of any choice of information type. For example, considering only positive feedback on the one hand, BM attacks can be prevented because malicious nodes would not be able to affect the trust level of trustworthy nodes by propagating negative reputation ratings. However, malicious nodes can collude and falsely praise misbehaved nodes to launch BS attacks. Propagating positive feedback also exhausts the network's limited resources since the number of nodes that behave correctly in general is supposed to be larger than those which do not. Thus, the number of transmissions required to update reputation values is high, which depletes the limited energy source.

Information Gathering Approach: Most current reputation systems in WSNs use monitoring mechanisms such as the Watchdog mechanism (WDM) [25] as an approach to collect these direct observations. When a node forwards a packet, the node's WDM verifies that the next node in the path also forwards the packet. Once there is a match, the packet is removed from the buffer. If the packet has remained in the buffer for longer than a certain timeout, the WDM increments a failure tally for the node which is responsible for forwarding the packet.

Reputation System Scope: Most of existing reputation-based trust systems focus on specific functions. For example, CONFIDANT [13] focus on detecting misbehaviors related to routing functionalities. It is important to know that reputation-based trust systems with different scopes make the comparison be-

tween these systems difficult. This is because a scope-specific reputation system requires the WDM to be tailored in order to monitor activities related to the chosen scope. For example, the aggregation scope requires the WDM to monitor routing, forwarding, sensing, and aggregation activities where each activity may use different reputation information type, while the localization scope requires the WDM to focus only on the provided location information.

4.2 Information Modeling Phase

This phase helps to calculate reputation values for such a node from the available information, which are provided by the previous phase. This phase is composed of two components as follows:

Information Modeling Structure: Reputation systems can be designed to calculate reputation values via a centralized, distributed, or a hybrid approach. In the centralized one, observations about a node's performance are propagated to a central authority that collects these observations, derives reputation values for each node and subsequently updates nodes with new reputation values. This approach relies on some assumptions, namely nodes completely trust the centralized authority which in turn must be correct and always available. However, if this approach is not carefully designed, it can become a single point of failure for the whole system. Also, this approach suffers from the lack of scalability, especially if the information is obtained from high latency sources. In the domain of WSNs, most recent applications were designed with a central robust authority, base station, in place. However, propagating observations across the network to the central point is impractical due to the scalability issue and the huge energy consumption. One way to minimize the energy consumption is by considering the distributed structure for information modeling.

In the distributed approach, each node propagates its observations to neighbors and then these nodes calculate the reputation values individually. Finally, reputation values in the hybrid approach are calculated by more than one entity.

Information Modeling Approach: This approach can be either deterministic or probabilistic. In the former, the output is uniquely determined by the input with no existence for randomness while the output, in the latter, can be predicted only within certain errors due to some randomness resources added to the input. The Bayesian model [8], for example, uses a probabilistic approach, which is Bayes formula, to model the reputation information. On the other hand, the majority vote used in Srinivasan et al.'s system [15] is an example for deterministic information modeling approach. In this voting approach, a sensor node calculates the reputation value of a specific beacon node by summation the positive and negative votes reported by neighboring beacon nodes.

4.3 Decision Making Phase

This phase helps to decide based on available reputation information whether or not the trustworthiness of a specific node is enough for a certain interaction or task. The decision metric can be either binary, discrete, or continuous. In the binary decision metric, the cooperate and do not cooperate decisions are represented by two symbols 1 and 0, respectively. This is usually based on a threshold policy, which is common in most reputation-based trust systems for WSNs. If

the reputation value of a sensor node is above a predefined threshold, then cooperation with this node is preferable. If a trust model provides more information about the trustworthiness of an entity, e.g., the trustworthiness comes from a set of discrete values (e.g., distrusted, uncertain, trusted, very trusted) or continuous values (e.g., in the range of [0,1]), then the final decision, whether to interact with an entity or not, can be done in a more sophisticated way. For example, if the trust value can be interpreted as a probability of a successful interaction and if it is possible to assign values for utilities and costs to a successful and unsuccessful interaction, respectively, then one might apply utility-based decision making for deciding whether it is rational to interact or not [28, 29].

4.4 Dissemination Phase

This phase helps to ensure that the decision resulted from the previous phase is available at each neighbor. This phase is composed of two components as follows:
Dissemination Structure: The dissemination structure can be either a distributed or centralized structure. In the former, each node calculates reputation values of other nodes in the neighborhood, stores them locally, and then shares them with its neighbors. This type of structure helps nodes being updated about other nodes by quickly filling their reputation tables. However, redundancy in this reported reputation information exists, which affects the limited energy source in nodes. Unfortunately, the distributed structure opens doors for an adversary to affect the reputation values by launching BS, BM, or OO attacks. Consequently, system designers should carefully pay attention when they follow this structure. In the latter, calculated reputation values are stored and distributed by a single entity. However, this entity has to have greater resources (enough memory and enough energy) to manage the dissemination activities.
Dissemination Approach: It can be either proactive or reactive. In the former, reputation values are broadcasted periodically, although there are no changes to reputation values since last update. In the latter, reputation values are only broadcasted when there are sufficient changes to these reputation values. Proactive dissemination, on the one hand, is suitable for resource constraint devices in busy networks, because reputation values are updated regularly for more than one activity. This helps reduce the number of transmissions required to update reputation values. On the other hand, reactive dissemination is suitable in networks with light traffic where reputation information is disseminated only on request. This helps minimize the number of transmissions in cases where there are no sufficient changes in the reputation values. It also covers designs where reputation values are piggy-backed on reply messages such as in CORE [30].

5 Comparison of Current Reputation-based Systems

This section provides the security and performance analysis of existing reputation-based trust systems in WSNs. It is believed that this analysis is not easy for the following reasons:

- There is no standard adversarial model where current reputation-based trust systems compete to provide a higher level of security, or resilience to attacks.
- Most current reputation-based trust systems did not cover all reputation components, which sometimes makes the comparison infeasible.

Thus, existing reputation-based trust systems are compared in a number of different ways: reputation components the systems are composed of, and resilience against attacks described in Section 3.

5.1 Reputation Components Visibility

According to the discussion in Section 4, reputation-based trust systems often share similar structural pattern. They consist of four main phases: information gathering and sharing, information modeling (or reputation calculation), decision making, and dissemination (see Figure 3). This section investigates the visibility of these phases (and the internal components of each phase) in the existing reputation-based trust systems. Current reputation based trust systems in WSNs are designed in order to enhance the trustworthiness between sensor nodes. These systems fall under one of five categories (scopes): generic, localization, mobility, routing, and aggregation. The systems on Table 1 and Table 2 are selected as representatives for these five scopes. Table 1 also incorporates the discussion on Section 4 and then analyzes trust systems designed for WSNs. It depicts the information related to each phase (and its components) covered by the designers of each trust system, which helps understanding the differences between the reputation-based trust systems in the current literature. It is believed that Table 1 is self-explanatory and hence no discussion is provided about it.

5.2 Attack Visibility

This section helps to determine whether or not these systems are vulnerable to attacks discussed in Section 3. Damage caused by these attacks varies from no damage in one system to maximum damage in another one, depending on the security assumptions used and whether these attacks were considered at the design time or not. Table 2 shows that attacks are less visible in Boukerche et al.'s system [26], because of the assumption on the secure deployment of mobile agents. Boukerche et al.'s assumed that these agents are generated and launched by a trusted authority, and are not subjected to node compromise attacks, which is an unrealistic assumption. We agree with Shaikh et al. [10] that Boukerche et al.'s system [26] is not well suited for realistic WSNs. It is believed that more attacks will threaten their system if the assumption is relaxed.

The Selective Forwarding (SF) attack occurs when an adversary, which is controlling a compromised node, selectively forwards received messages. Unfortunately, all systems in Table 2 are vulnerable to the SF attack, because launching node compromise attacks against the current version of sensors is trivial. The damage caused to reputation systems by the SF attack varies from partial damage to maximum damage as shown in Table 2. The SF attack causes partial damage in systems [10–14, 17, 25, 26, 31, 33] although they monitor the forwarding activity. This is because most of these systems use a binary decision method when they evaluate the trust level of a specific node. This method is based on a threshold policy, and once the node's reputation is above this threshold value, then the node is considered trusted. The damage is considered partial because of adjusting the threshold value or applying mechanisms such as ageing factor and weighting can help defeating this attack. Unfortunately, some systems designers

Schemes	Gathering & Sharing				Calculation		Decision	Dissemination	
	Source	WDM	Type	Scope	Structure	Approach	Metric	Structure	Approach
Michiardi & Molva [25]	D/I	Y	+	R	D_i	?	?	D_i	R_e
Buchegger & Boudec [13]	D/I	Y	-	R	D_i	?	B	D_i	R_e
Ganeriwal & Srivastava [34]	D/I	Y	+	G	D_i	P_r	B	D_i	P
Srinivasan et al. [14]	D	Y	+,-	M	C	P_r	?	C	R_e
Boukerche et al. [26]	D	N	+,-	G	P2P	?	?	P2P	R_e
Alzaid et al. [11]	D	Y	-	A	D_i	P_r	B	D_i	R_e
Yao et al. [17]	D/I	Y	+,-	G	D_i	D_e	Disc	D_i	R_e
Shaikh et al. [10]	D/I	?	+,-	G	H	D_e	Disc	H	P, R_e
Özdemir [33]	D/I	Y	+,-	A	D_i	P_r	B	D_i	P
Bouckerche & Ren [12]	D/I	?	+,-	M	C	D_e	B	C	P, R_e
Chen et al. [31]	D	Y	+,-	R	D_i	P_r	B	D_i	P
Chen [32]	D	Y	?	G	D_i	P_r	?	?	?
Xiao et al. [16]	D/I	?	+,-	G	D_i	P_r	B	D_i	?
Srinivasan et al. [15]	D/I	Y	+,-	L	D_i	D_e	?	D_i	R_e
Chen et al. [35]	D	Y	+,-	G	D_i	P_r	D_i	?	?
Sen & Krishna. [36]	D	Y	+,-	G or M	P2P	D_e	B	P2P	P, R_e
Crosby et al. [37]	D	N	-	L	?	P_r	B	?	?
Perez-Toro et al. [38]	D/I	?	+/-	A	D_i	P_r	B	D_i	P

D	Automatic Direct	**+**	Positive Feedback	**A**	Aggregation Misbehavior	$\boldsymbol{D_i}$	Distributed
I	Automatic Indirect	**-**	Negative Feedback	**?**	Not available	**Disc**	Discrete
WDM	Watchdog Mechanism	$\boldsymbol{R_e}$	Reactive	**G**	Generic Misbehavior	**M**	Mobility
C	Centralized	**P**	Proactive	**Y**	Yes	**P2P**	Peer to Peer
H	Hybrid	**B**	Binary	**N**	No	**R**	Routing Misbehavior
$\boldsymbol{P_r}$	Probabilistic	**L**	Localization Misbehavior	$\boldsymbol{D_e}$	Deterministic		

Table 1. The visibility of reputation components in current reputation-based trust systems

Schemes	WSNs Attacks				Reputation Attacks			
	SF	SY	SD	RE	BM	BS	OO	NC
Michiardi & Molva [25]	•		••	••		••	•	
Buchegger & Boudec [13]	•	••	•	••	••		••	••
Ganeriwal & Srivastava [34]	•		••	••		••	••	•
Srinivasan et al. [14]	•	••	•	••			•	••
Boukerche et al. [26]	•		•				•	
Alzaid et al. [11]	•		•				••	
Yao et al. [17]	•	••	••		••	••	••	••
Shaikh et al. [10]	•		•		•	•	••	
Özdemir [33]	•		••	••	••	••	••	
Bouckerche & Ren [12]	•		•	••	••	••	••	
Chen et al. [31]	•	••	••	••			••	••
Xiao et al. [16]	••	••	••	••	••	••	••	••
Srinivasan et al. [15]	••		••	••	••	••	••	

	Robust
•	Partial damage
••	Maximum damage

Table 2. Attacks visibility in current reputation-based trust systems

did not consider forwarding misbehaving in their systems such as in [15, 16] and therefore, the damage caused by the SF attack is maximum.

Table 2 shows that there is a link between the adversary capability of launching Sybil (SY) and Newcomer (NC) attacks. According to the discussion in Section 3, the adversary can launch the SY attack by presenting more than one identity, which means that the adversary is able to launch NC attack once it has succeeded in presenting another identity beside its original identity. Interestingly, reputation-based trust systems such as [13, 14, 16, 17, 31] are vulnerable to SY and NC attacks. This is due to the lack of discussion on an authentication process used between sensor nodes in these systems.

The Replay (RE) attack occurs if an adversary is able to replay old messages into the network. Surprisingly, this attack is visible in reputation-based trust systems such as [12–16, 31]. Other systems [10, 11, 17, 26] are considered robust against RE attacks because mechanisms such as nonces and timestamps are used in order to defeat the attack. It is argued that systems with vulnerability to the RE attack, are also vulnerable to the Spoofed Data (SD) attack because the adversary can first capture some reputation information in understandable format and then replay it into the network after changing it, in order to affect the performance of the reputation component; which is one form of the SD attack.

Bad Mouthing (BM) and Ballot Stuffing (BS) attacks are visible in systems that use indirect observations in the reputation calculation phase. Consequently, systems in [11, 14, 26, 31] are robust against BM and BS attacks, because sharing direct observations with neighbors is prohibited. The BM attack is visible

in reputation-based trust systems that allow nodes to exchange their negative feedback such as in [10, 12, 13, 15–17, 33]. On the other hand, the BS attack is visible in systems that allow nodes to propagate their positive feedback such as in [10, 12, 15–17, 25, 33]. The damage caused by BM and BS is partial in [10], because indirect observation is considered in reputation calculation only if past communication experience does not exist or not enough to determine the trustworthiness of a specific node.

The On-Off (OO) attack occurs when the adversary tries to launch a mixture of attacks discussed in Section 3 in an irregular basis in order to keep its reputation value within an acceptable trust value. Importantly, Table 2 shows that all reputation-based trust systems are vulnerable to this attack. The damage caused by this attack varies, depending on how many other attacks the system is vulnerable to.

6 Conclusion

This paper provides a detailed review of reputation-based trust systems in wireless sensor networks. It first explains the motivation behind adding the reputation system capabilities into wireless sensor networks, which in brief helps to enhance the trustworthiness among sensor nodes. It then discusses how the integration between wireless sensor networks and reputation systems can open doors for an adversary to threaten those reputation-based trust systems destined for wireless sensor networks, and hence affect the entire performance. After that, the "state-of-the-art" in reputation-based trust systems is surveyed and classified into five categories: generic, localization, mobility, routing, and aggregation depending on what activity attracts most the system designers. Subsequently, current reputation-based trust systems in wireless sensor networks are compared in a number of different ways: the reputation components they are composed of, and the attacks they secure against.

References

1. Murthy, C. S. R., Manoj B.S.: Ad Hoc Wireless Sensor Networks Architectures and Protocols. Prentice Hall PTR, Upper Saddle River, NJ, USA (2004)
2. Guimarães, G., Souto, E., Sadok, D. F. H., Kelner, J.: Evaluation of Security Mechanisms in Wireless Sensor Networks. In: Proceedings of the International Conference on Wireless Technologies/High Speed Networks/Multimedia Communications Systems/Sensor Networks, ICW/ICHSN/ICMCS/SENET, pp. 428–433. Montreal, Canada (2005)
3. Hartung, C., Balasalle, J., Han, R.: Node Compromise in Sensor Networks: The Need for Secure Systems. Technical Report, CU-CS-990-05. University of Colorado at Boulder - Department of Computer Science (2005)
4. Yan, Z., Zhang, P., Virtanen T.: Trust Evaluation Based Security Solution in Ad hoc Networks. (2003), `http://research.nokia.com/publications/trust_evaluation_based_security_solution_ad_hoc_networks`.
5. Dasgupta, P.: Trust As a Commodity: Trust Making and Breaking Cooperative Relations. In: Gambetta, D. (eds.), 3rd ed. pp. 49–72. Basil Blackwell Publishing Ltd, Oxford, UK (2000)
6. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision Support Systems. vol. 43, no. 2, pp. 618–644 (2007)

7. Keser, C.: Experimental games for the design of reputation management systems. IBM Systems Journal. vol. 42, no. 3, pp. 498–506 (2003)
8. Ismail, R., Jøsang, A.: The beta reputation system. In: Proceedings of the 15th Bled Conference on Electronic Commerce (2002)
9. Golbeck, J. A.: Computing and applying trust in web-based social networks. Ph.D. dissertation, College Park, MD, USA. The thesis is retrieved 24th of May 2012 (2005)
10. Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee H., Lee, S., Song, Y. J.: Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems. vol. 20, no. 11, pp. 1698–1712 (2009)
11. Alzaid, H., Foo, E., Nieto, J. G.: RSDA: Reputation-Based Secure Data Aggregation in Wireless Sensor Networks. In: Proceedings of the 9^{th} International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT'08, pp. 419–424. Dunedin, New Zealand (2008)
12. Boukerche, A., Ren, Y.: A trust-based security system for ubiquitous and pervasive computing environments. Computer Communications. vol. 31, no. 18, pp. 4343–4351 (2008)
13. Buchegger, S., Boudec, J.-Y. L.: Performance analysis of the CONFIDANT protocol. In: Proceedings of the 3^{rd} ACM international symposium on Mobile ad hoc networking and computing, MobiHoc'02, pp. 226–236. Lausanne, Switzerland (2002)
14. Srinivasan, A., Li, F., Wu, J.: A Novel CDS-Based Reputation Monitoring System for Wireless Sensor Networks. In: Proceedings of the 28^{th} IEEE International Conference on Distributed ComputingSystems Workshops, ICDCS'08, pp. 364–369. Beijing, China (2008)
15. Srinivasan, A., Teitelbaum, J., Wu, J.: DRBTS: Distributed Reputation-based Beacon Trust System. In: 2^{nd} International Symposium on Dependable Autonomic and Secure Computing, DASC'06, pp. 277–283. Indianapolis, Indiana, USA (2006)
16. Xiao, D., Feng, J., Zhang, H.: A formal reputation system for trusting wireless sensor network. Wuhan University Journal of Natural Sciences. vol. 13, no. 2, pp. 173–179 (2008)
17. Yao, Z., Kim, D., Doh, Y.: PLUS: parameterised localised trust management-based security framework for sensor networks. IJSNET. vol. 3, no. 4, pp. 224–236 (2008)
18. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks. vol. 1, no. 2-3, pp. 293–315 (2003)
19. Michiardi, P., Molva, R.: Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. European Wireless Conference (2002)
20. Kifayat, K., Merabti, M., Shi, Q., Llewellyn-Jones, D.: Security in Wireless Sensor Networks: Handbook of Information and Communication Security. In: Stamp, M., Stavroulakis, P.r (eds). ch. 26, pp. 513–552, Springer Berlin Heidelberg (2010)
21. Alzaid, H., Foo, E., Nieto, J. M. G.: Secure data aggregation in wireless sensor network: A survey: In: Proceedings of the 6^{th} Australasian conference on Information security,AISC'08, pp. 93–105. Wollongong, NSW, Australia (2008)
22. Ismail, R.: Security of Reputation Systems. Ph.D. dissertation, Queensland University of Technology, Brisbane, Australia. The thesis is retrieved 24th of May 2012 (2004)
23. Jøsang, A., Golbeck, J., Challenges for Robust Trust and Reputation Systems. In: Proceedings of the 5th International Workshop on Security and Trust Management (STM'09), pp. 1–6. Saint Malo, France (2009)
24. Feldman, M., Chuang, J.: Overcoming free-riding behavior in peer-to-peer systems. SIGecom Exchanges. vol. 5, no. 4, pp. 41–50 (2005)

25. Michiardi, P., Molva, R.: CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Communications and Multimedia Security. vol. 228, pp. 107–121 (2002)
26. Boukerche, A., Xu, L., El-Khatib, K.: Trust-based security for wireless ad hoc and sensor networks. Computer Communications. vol. 30, no. 11-12, pp. 2413–2427 (2007)
27. Jøsang, A., Luo, X., Chen, X.: Continuous Ratings in Discrete Bayesian Reputation Systems: In: Proceedings of the 2^{nd} Joint iTrust and PST Conference on Privacy, Trust Management and Security, pp. 151–166. Saint Malo, France (2008)
28. Bernoulli, D.: Exposition of a New Theory on the Measurement of Risk. Econometrica. vol. 22, no. 1, pp. 23–36 (1954). http://dx.doi.org/10.2307/1909829
29. Morgenstern, O., Neumann, J. V.: Theory of Games and Economic Behavior. Princeton University Press, New York (1980)
30. Marti, S., Giuli, T. J., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6^{th} annual international conference on Mobile computing and networking, MOBICOM, pp. 255–265. Boston, Massachusetts, United States (2000)
31. Chen, H., Wu, H., Hu, J., Gao, C.: Agent-Based Trust Management Model for Wireless Sensor Networks. In Proceedings of the International Conference on Multimedia and UbiquitousEngineering, MUE'08, pp. 150–154. Busan, Korea (2008)
32. Chen, H.: Task-based Trust Management for Wireless Sensor Networks. International Journal of Security and its Applications. vol. 3, no. 2, pp. 21–26 (2009)
33. Özdemir S.: Functional Reputation Based Data Aggregation for Wireless Sensor Networks. In: Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob'08, pp. 592–597. Avignon, France (2008)
34. Ganeriwal, S., Balzano, L. K., Srivastava, M. B.: Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks. vol. 4, no. 3, pp. 1–37 (2008)
35. Chen, H., Wu, H., Zhou, X., Gao, C.: Reputation-based Trust in Wireless Sensor Networks. In: Proceedings of the International Conference on Multimedia and Ubiquitous Engineering, MUE'07, pp. 603–607. Seoul, Korea (2007)
36. Sen, J., Krishna, S.: An Efficient Security Mechanism for High-Integrity Wireless Sensor Networks. CoRR. vol. abs/1111.0380 (2011)
37. Crosby, G. V., Hester, L., Pissinou, N.: Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks. International Journal on Network Security. vol. 12, no. 2, pp. 107–117 (2011)
38. Perez-Toro, C., Panta, R., Bagchi, S.: RDAS: Reputation-Based Resilient Data Aggregation in Sensor Network. In: Proceedings of the 7^{th} Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks, SECON, pp. 1–9. Boston, Massachusetts, USA (2010)