http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (22): 6686-6693, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.6686.6693

Reasoning about Trust and Reputation System to Coordinate Wireless Sensor Networks

Qiang Yang
Computer School Yangtze University, Jingzhou 434023, China

Abstract: Due to the nature of the WSN and the extreme resource constraints of sensor devices, providing secure, efficient and user-friendly trust initialization is a challenging task. This study identify a coordination communication model which characterizes trust groups in order to promote safe interactions in the ubiquitous environment. Through the proposed TRSCM (Trust and Reputation System for Communication Management), a group of sensor devices that have no pre-shared secrets, establish initial trust by generating various shared secret keys out of an unauthenticated channel. The dynamics of trust group creation, evolution and termination are described, in terms of the history of interactions of the device and on the ontology used to encode the context of trust. After the reasoning the security of the proposed protocols, we implement the middleware on a network testbed and report performance evaluation results.

Key words: Turst management, wireless sensor networks, intrusion detection, reputation

INTRODUCTION

The concept of trust has become very relevant in the late years as a consequence of the growth of fields such as internet transactions or electronic commerce (Harvard University, 2013; University of Cambridge, 2012). In general, one of the most difficult challenges of the mobile ad-hoc environment has not received much attention yet, that is, how to decide who to trust in this plethora of opportunistically connected peers (FIRE, 2013; Sen and Sajja, 2002). Each time an interaction takes place, we face an inherent risk as we can never be certain of the trustworthiness of the entities we interact with, or that mediate the interaction (Alarifi and Du, 2006; Alcaraz and Roman, 2006; Beckwith *et al*., 2011; Blaze *et al*., 1996).

Wireless Sensor Network (WSN) has evolved into a useful network paradigm applicable to many existing problems, such as environmental and structural monitoring, e-Health and many others. A sensor nodes (SNs) deployed in the WSN has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing (Lawen, 2003; Liu *et al*., 2004). Wireless networks of broader bandwidth allow these mobile units to aggregate and form complex distributed system structures, thus providing users anytime-anywhere access to their personal information, as well as public resources and services (Ma and Tsudik, 2007; Manzo *et al*., 2005; Minder *et al*., 2005).

Trust management systems for WSN could be very useful for detecting misbehaving nodes (faulty or malicious) and for assisting the decision-making process. Very little has been done so far in the area of trust management systems for WSN (Chen *et al*., 2007; Crosby *et al*., 2006; Ganeriwal and Srivastava, 2004). Most of the work on this field has been made in the last few years. Big efforts, however, have been made in related areas such as P2P and Ad-Hoc networks (Josang and Ismail, 2002). Thus, some of the approaches adopted for WSN try to imitate those for Ad-hoc or P2P networks (Josang *et al*., 2007; Kamvar *et al*., 2003). A Trust Management Framework (TMF) offers a solution to the problem. It aims at reducing the uncertainty that characterizes mobile ad-hoc interactions by enabling devices to form, exchange and evolve trust opinions about other agents in the system. The size of the networks also becomes an issue. P2P networks are usually large in size of nodes whereas this is not always the case in WSN.

Related work: This gives rise to the problem of secure ad hoc initial trust establishment which happens before WSN is actually deployed (Karlof and Wagner, 2003; Karlof *et al*., 2004). Here we highlight several key differences between this and traditional key pre-distributions. (1) Since secret keys are not assumed to be pre-distributed, trust must be established despite the lack of a common security context and no central trusted parties as the root of trust except that the user trusts herself. In particular, in practice, a group of WSN devices must be correctly associated with the intended patient, lest the wrong medical data be collected. This requires the wireless nodes to be authenticated to each other and to the WSN controller which forms the group securely. Secret keys which can belong only to the intended group should be generated. (2) The traditional authentication

goal (Krasniewski *et al*., 2005; Park and Shin, 2010) only stipulates that each participant is assured that each message appears to come from the true identity that generated it. (3) WSN applications are usually time-critical which mandates the trust bootstrap process to be fast and scalable. For instance, in EMS an additional 5 minutes delay may result in a difference between life and death. Of course, overhead is an important concern since the medical sensor nodes are extremely resource-constrained. To date, most of the proposed solutions focus on providing support for subjective reasoning. In (Rebahi *et al*., 2005; Bearly and Kumar, 2004), a mechanism for the management of distributed reputation in mobile ad-hoc networks is presented, that is able to effectively detect malicious recommenders based on the idea of 'recommendation reputation', that is, agents are judged based on the recommendations they have given in the past (although trust and knowledge are still confused). Social control mechanisms have been proposed to automatically isolate malicious entities and exclude them from future interactions without having to rely on a trusted third party. While supporting subjective reasoning to different extents, none of the approaches outlined above attempts to model trust group reasoning. In (Becher *et al*., 2012), the formation of trusted coalitions of agents is discussed; however, the study presents very early work and ideas without details about how coalitions are actually formed and how they evolve.

System overview: The initial trust establishment during pre-deployment should establish a group key and/or individual keys shared between each sensor and the controller which can be used for the controller to securely broadcast messages to the later, such as queries. TRSCM (Trust and Reputation System for Communication Management) are proposed which promotes trust-aware collaborations in WSN by enabling each truster agent to collect and process trust information about a trustee agent b, so to forma trust opinion before interaction takes place. Sources of trust information are: direct experiences and recommendations.

Definition 1 (reliability trust): Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends.

This definition includes the concept of dependence on the trusted party and the reliability (probability) of the trusted party, as seen by the trusting party. The meaning of the tuple is as follows: agent a trusts agent bat level l∈[-1, 1] (-1 meaning total distrust and 1 meaning blind trust) to carry out services. For example, we may specify that Alice (a) trusts Bob's eBookshop (b) at level 0.8(l) to sell travel books (s).

Definition 2 (Direct experiences): The truster history of interactions with b is processed and kept locally in the form of a single aggregated trust information tuple: [a, b, l, s, k, t].

Because in mobile ad-hoc settings agents can have only a partial knowledge of their surroundings, their trust opinions contain a level of uncertainty. A compromised SN can perform various attacks including forgery attacks, jamming attacks, Sybil attacks, denial of service attacks, black/sink hole attacks (absorbing and dropping packets) and slandering attacks.

Definition 3 (Decision trust): Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.

The higher the number of direct experiences happened between the truster and the trustee, the higher the degree of knowledge. Reputation systems, on the other hand, assume that some participants will try to misrepresent the quality of services in order to make more profit and to lie or provide misleading ratings in order to achieve some specific goal.

Definition 4 (Reputation): Reputation is what is generally said or believed about a person's or thing's character or standing.

Agents are thus judged based on the quality of the recommendations they give, in the same way they are assessed for any other service they provide. The latter can cause problems, because most reputation systems will be unable to distinguish between variations in service provider performance and variations in the observer's taste, potentially leading to unreliable and misleading reputation scores.

Definition 5 (Recommendations): When direct experiences are not available (e.g., because no interaction has ever happened in the past between the truster and the trustee), the truster may ask other agents in the environment (what we call the social context) for recommendations. For example, Alice may be willing to buy books from Bob's eBook shop provided that it has been recommended by Clare (agent x). A recommendation tuple sent by x about agent b looks like: $[x, b, l, s, k, t]_{sk}$.

A recommendation is thus computed by signing the local aggregated tuple; a signature is necessary to prove the recommendation's authenticity. Practical factors need to be considered when choosing the type of OOB channel in a device pairing protocol.

Figure 1 shows TRSCM model overview. Commitment schemes are important cryptographic primitives that have been widely used in message authentication and authenticated key agreement protocols. Upon completion

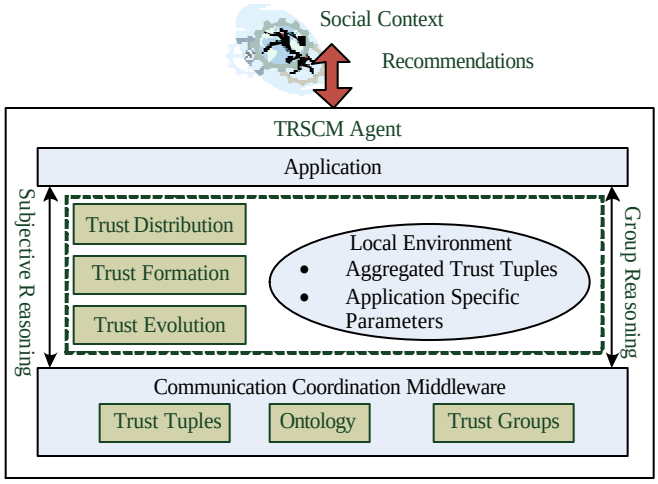

Fig. 1: TRSCM coordination middleware

of an interaction between a and b, the trust evolution component of agent a updates a local environment. For example when a contract specifies quality requirements for the delivery of services, then this business trust would be provision trust in our terminology.

Although enabling subjective reasoning, the social network model TRSCM is based on, that is, a flat collection of individual agents, is too simplistic and far from reality. In human interactions, we view the social network as a set of (possibly overlapping) communities and we most frequently coordinate with the communities we belong to. Factors for this type of trust can for example be critical infrastructures, insurance, legal system, law enforcement and stability of society in general. For example, when seeking for recommendations about a specific service provider, rather than querying the social network at large, we may query only the community of people that we know can provide us with useful information about it, thus increasing the quality of the information received(effectiveness) and reducing the number of recommendations that have to be processed (efficiency). In the following section, we illustrate how to model groups on top of a flat social network and how to exploit them to promote trust aware coordination.

The model described in the previous sections has been realized by means of the coordination middleware depicted in Fig. 2 (components that are not the focus of the study, such as discovery, are not shown). Trust purpose is an overarching concept that that can be used to express any operational instantiation of the trust classes mentioned above. Application developers engineer trust-based collaborations by means of two simple interfaces: an interface that enables subjective reasoning about individual agents and an interface that enables group reasoning.

Trust management for wireless sensor networks: In the pre-deployment phase, the sensor nodes are bootstrapped for the first time after being purchased; thus, initial trust among sensors should be established in this phase. For sensor networks it is possible to define the structure of a generic trust entity, as shown in Fig. 2. Conceptually, identity trust and provision trust can be seen as two layers on top of each other, where provision trust normally can not exist without identity trust.

In the absence of identity trust it is only possible to have a baseline provision trust in an agent or entity. The idea behind trust transitivity is that when Alice trusts Bob and Bob trusts Claire and Bob refers Claire to Alice, then Alice can derive a measure of trust in Claire based on Bob's referral combined with her trust in Bob. This is illustrated in Fig. 2.

Trust-based geographic routing and intrusion detection: In flooding-based routing, a node floods a message to all its neighbors until a copy of the packet reaches the destination node. It yields the highest message delivery ratio and the lowest message delay at the expense of the highest message overhead.

In this section, we apply the proposed hierarchical trust management protocol to trust-based geographic routing as an application.

Definition 6 (Geographic routing): A node disseminates a message to a maximum of L neighbors closest to the

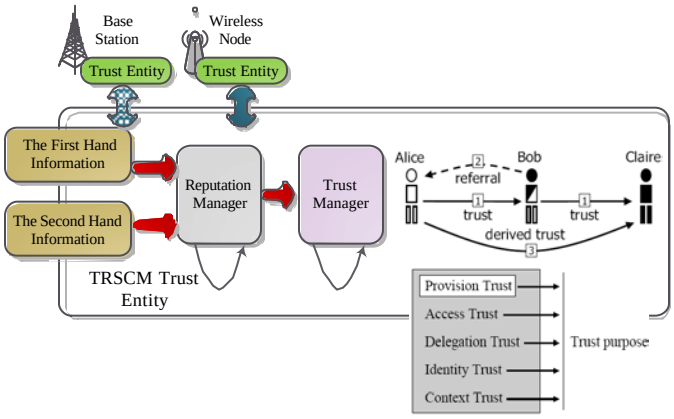

Fig. 2: Trust Entity Structure for WSN

destination node (or the sink node). In trust-based geographic routing, node i forwards a message to a maximum of L neighbors not only closest to the destination node but also with the highest trust values $T_{ij}(t)$. We conduct a performance analysis to compare our trust-based geographic routing protocol with baseline routing protocols, namely, flooding-based and traditional geographic routing.

The central authority (reputation centre) that collects all the ratings typically derives a reputation score for every participant and makes all scores publicly available. Then, the CH forwards the message to the sink node through other CHs. Without loss of generality, we normalize the average delay for forwarding a message between two neighbor nodes to τ. The average delay between two neighbor nodes is normalized to 2τ. We collect data for delivering 1000 messages, each with a source sensor and a sink node randomly selected. We consider two cases: L = 1 and L = 2 for both trust-based geographic routing and geographic routing. In the comparative analysis, we vary the degree of selfish or compromised nodes from 0 to 90%. Note that 30% of compromised or selfish nodes means that 30% of nodes are compromised or selfish in the system without a fixed ratio being used for these two types of nodes. We use parameter values for characterizing environmental and operational conditions. We also use the optimal set of (α, β) for each individual trust property to ensure subjective trust is close to objective trust.

Participants can then use each other's scores, for example, when deciding whether or not to transact with a particular party. We first describe the algorithm that can be used by a high-level node such as a node (or a base station) to perform trust-based intrusion detection under its control. Then we develop a statistical method to assess trust based IDS false positive and false negative probabilities.

The idea is that transactions with reputable participants are likely to result in more favorable outcomes than transactions with disreputable participants. A similar treatment applies to a base station performing trust-based intrusion detection on base station in a WSN.

Algorithm for trust-based intrusion detection

Definition 4: A cluster head node performs cluster head -to-node trust evaluation toward node j after receiving T_{ij} (t) values from all nodes in the cluster. More specifically a cluster head node, c, when evaluating a node, j, willcompute node j's trust value, $T_{cj}(t)$. cluster head c will announce node j as compromised if T_{cj} (t) is less than T^{th}; otherwise, node j is not compromised.

Statistical analysis: Consider that the value toward node j is a random variable following normal distribution commonly used for statistical analyses with mean value $\mu_{ij}(t)$. Also consider that there are n sample values of T_{ij} (t) submitted by n nodes considered trustworthy by the cluster head. With these n sample values, X_j (t) is related to the sample mean, sample standard deviation and true mean following t-distribution with n-1 degree of freedom as follows:

$$X_j(t) = \frac{\overline{T_{ij}(t)} - \mu_j(t)}{S_j(t)/\sqrt{n}} \quad (1)$$

where, $\overline{T_{ij}(t)}$, S_j (t) and μ_j (t) are the sample mean, sample standard deviation and true mean of node j's trust value at time t, respectively. Thus, the probability that node j is diagnosed as a compromised node at time t is:

$$\Theta_j(t) = \Pr(\mu_j(t) < T^{th}) = \Pr\left(X_j(t) > \frac{\overline{T_{ij}(t)} - \mu_j(t)}{S_j(t)/\sqrt{n}} \right) \quad (2)$$

The false positive of the IDS can be obtained by calculating $\Theta_j(t)$ under the condition that node j is not compromised. Similarly, the false negative probability can be obtained by calculating $1-\Theta_j(t)$ under the condition that node j is compromised:

$$P_j^{fp}(t) = \Pr\left(X_j(t) > \frac{\overline{T_{ij}^N(t)} - \mu_j(t)}{S_j^N(t)/\sqrt{n}} \right) \quad (3)$$

$$P_j^{fn}(t) = \Pr\left(X_j(t) \le \frac{\overline{T_{ij}^C(t)} - \mu_j(t)}{S_j^C(t)/\sqrt{n}} \right) \quad (4)$$

The above give the false positive probability, $P_j^{fp}(t)$ and false negative probability, $P_j^{fn}(t)$, of our proposed trust-based intrusion detection algorithm at time t, respectively. $\overline{T_{ij}^N(t)}$ and $S_j^N(t)$ are the mean value and standard deviation of node j's trust values reported by other nodes in the same cluster, und $S_j^C(t)$ er the condition that node j is not compromised. $\overline{T_{ij}^C(t)}$ and are the mean value and standard deviation, under the condition that node j is compromised. $T_{ij}^N(t)$ and $T_{ij}^C(t)$ can be easily obtained by applying the Bayes theorem to the calculation of $T_{ij}(t)$.

$P_j^{fp}(t)$ and $P_j^{fn}(t)$ vary over time. The average false positive and false negative probabilities, denoted by $P_j^{fp}(t)$ and $P_j^{fn}(t)$ can be obtained by weighting on the probability of node j being compromised at time t, i.e.:

$$P_j^{fp} = \frac{\sum_{t=0}^{SL}\left(P_j^{fp}(t)(1-P_j^C(t))\right)}{\sum_{t=0}^{SL}(1-P_j^C(t))} \quad (5)$$

$$P_j^{fn} = \frac{\sum_{t=0}^{SL}\left(P_j^{fn}(t)(1-P_j^C(t))\right)}{\sum_{t=0}^{SL}P_j^C(t)} \quad (6)$$

where, $P_j^C(t)$ is the probability that node j is compromised at time t which can be obtained from the SPN model output and SL is the anticipated WNS lifetime period over which the weighted calculation is performed.

Intrusion detection analysis: We perform a comparative performance analysis of our trust-based intrusion detection algorithm with two anomaly detection schemes, namely, weighted summation and data clustering. We use the ROC (Receiver Operating Characteristic) curve as the performance metric since both false negative probability (P_{fn}) and false positive probability (P_{fp}) are critical measures and ROC objectively reflects the sensitivity of detection probability (i.e., $1-P_{fn}$) as the false positive probability varies.

The second baseline anomaly detection scheme is fixed width data clustering-based IDS. In this approach, the maximum radius of a cluster (c_w) is defined and a data point is put into a cluster if the distance between the centroid of the cluster and this data point is smaller than c_w; otherwise this data point makes a new cluster. Data points that exhibit dissimilarity with others will tend to cluster into a small cluster or standalone by themselves. These lone data points are reported as malicious.

In our trust-based intrusion detection algorithm, the false positive and negative probabilities essentially depend on the minimum trust threshold (T^{th}) and the weight of social trust (w_{social}). We vary these two parameters over the range of [0, 1] to collect the performance results.

Evalution

Best trust formation to maximize application performance: Here we identify the best way to form trust out of social and QoS trust properties (i.e., identifying weights to assign to individual trust properties) and to assign the minimum trust threshold, T^{th}, so that the performance of trust-based intrusion detection is maximized, i.e., both false positives and false negatives are minimized. Trust and reputation can be represented as linguistically fuzzy concepts, where membership functions describe to what degree an agent can be described as e.g. trustworthy or not trustworthy.

Fig. 3 shows max (P_{fp}, P_{fn}) vs. T^{th} and w_{social} in this system as a result of executing our trust-based intrusion detection algorithm, where P_{fp} and P_{fn} are the time-averaged false positive and false negative probabilities as calculated, respectively, over all nodes in the system. We observe that as the minimum trust threshold T_{th} increases, the false negative probability P_{fn} decreases while the false positive probability P_{fp} increases. More importantly, there exists an optimal trust threshold $T^{th, opt}$ at which both false negative and false positive probabilities are minimized. As trust formation affects how trust is formed from social and QoS trust components, we also observe that $T^{th, opt}$ is sensitive to w_{social}. Fig. 7 identifies that for the example WSN when $T^{th, opt}$ and w_{social} = 0.6, both false positive and false negative probabilities are minimized to fall below 5%.

Dynamic trust management: Fig. 4 is for the case in which the expected system lifetime SL is 150 days of operations. Fig. 8 shows the optimal trust threshold $T^{th,opt}$ = 0.6 as SL varies. Here, the value of wsocial is fixed

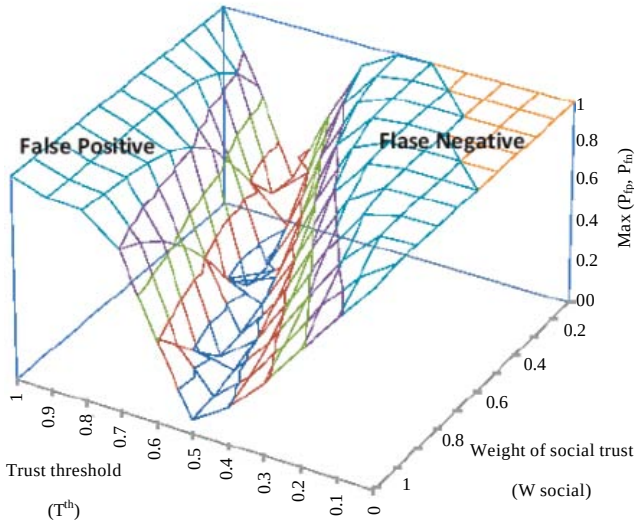

Fig. 3: Effect of and *wsocial* on *max*(*Pfp, Pfn*)

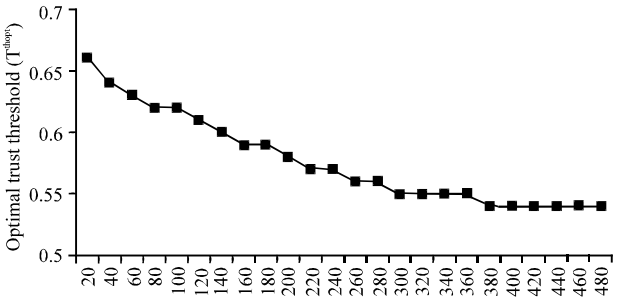

Fig. 4: ptimal trust threshold vs. system lifetime

to 0.6 to isolate its effect. For a WSN with a prolonged operation, each SL value represents a time point characterized by a distinct hostility level such as the percentage of compromised and selfish nodes. We observe that as SL increases, the value of $T^{th,opt}$ = 0.6 at which the false alarm probability is minimized decreases. The reason is that a node's trust value decreases over time due to energy depletion even if the node is not compromised. The system sensing hostility change at runtime can apply the best w_{social} and $T^{th,opt}$ = 0.6 setting identified from static analysis to optimize application performance in false alarm probability.

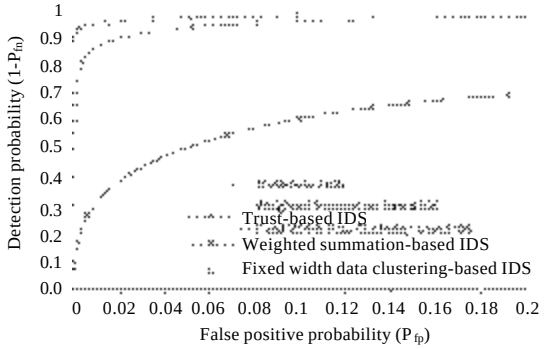

Fig. 5: Performance comparison of IDS schemes in detection probability vs. false positive probability.

Detection probability with false positive probability: In Fig. 5 we compare the ROC curves of our trust-based IDS algorithm against those by weighted summation-based IDS and fixed width data cluster-based IDS for SL = 240 days. Instead, there can be distributed stores where ratings can be submitted, or each participant simply records the opinion about each experience with other parties and provides this information on request from relying parties. We observe that as a design tradeoff, as

the false positive probability increases, the detection probability increases for all IDS schemes. After each transaction, the agents provide ratings about each other's performance in the transaction. The reputation centre collects ratings from all the agents and continuously updates each agent's reputation score as a function of the received ratings. The strength of our trust-based IDS algorithm is especially pronounced when the false positive probability approaches zero. This is very desirable since our trust-based IDS algorithm can still maintain a high detection probability (>90%) when the false positive probability is close to zero at which the detection probability of anomaly detection-based IDS schemes drops sharply.

CONCLUSION

In this study, we proposed a dynamic trust management protocol for wireless sensor networks, considering two aspects of trustworthiness, namely, social trust and QoS trust. Updated reputation scores are provided online for all the agents to see and can be used by the agents to decide whether or not to transact with a particular agent. Our trust-based IDS algorithm outperforms traditional anomaly-based IDS techniques in the detection probability while maintaining sufficiently low false positives. Theory of probabilities and some theories developed for these purposes such as the belief theory provide a well founded mathematical tool for trust management systems in general. Although group management requires some additional resource consumption over non group-based solutions it later simplifies an agent's reasoning about which other agents to deal with, thus actually achieving more efficient and effective coordination.

REFERENCES

Alarifi, A. and W. Du, 2006. Diversify sensor nodes to improve resilience against node compromise. Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, October 30, 2006, Alexandria, USA., pp: 101-112.

Alcaraz, C. and R. Roman, 2006. Applying key infrastructures for sensor networks in cip/ciip scenarios. Proceedings of the 1st International Workshop on Critical Information Infrastructures Security, August 31-September 1, 2006, Samos, Greece, pp: 166-178.

Bearly, T. and V. Kumar, 2004. Expanding trust beyond reputation in peer-to-peer systems. Proceedings of the 15th International Workshop on Database and Expert Systems Applications, August 30-September 2, 2004, Zaragoza, Spain, pp: 966-970.

Becher, A., Z. Benenson and M. Dornseif, 2012. Tampering with motes: Real-world physical attacks on wireless sensor networks. Proceedings of the 3rd International Conference on Security in Pervasive Computing, April 1-3, 2012, UK., pp: 104-118.

Beckwith, R., D. Teibel and P. Bowen, 2004. Report from the field: Results from an agricultural wireless sensor network. Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, November 16-18, 2004, Tampa, USA., pp: 471-478.

Blaze, M., J. Feigenbaum and J. Lacy, 1996. Decentralized trust management. Proceedings of the IEEE Symposium on Security and Privacy, May 6-8, 1996, Oakland, CA., USA., pp: 164-173.

Chen, H., H. Wu, X. Zhou and C. Gao, 2007. Reputation-based trust in wireless sensor networks. Proceedings of the International Conference on Multimedia and Ubiquitous Engineering, April 26-28, 2007, Seoul, South Korea, pp: 603-607.

Crosby, G.V., N. Pissinou and J. Gadze, 2006. A framework for trust-based cluster head election in wireless sensor networks. Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems, April 24-28, 2006, Columbia, MD., USA., pp: 10-22.

FIRE, 2013. FIRE project 2013. University of California, Berkeley, USA.

Ganeriwal, S. and M. Srivastava, 2004. Reputation-based framework for high integrity sensor networks. Proceedings of the 2nd ACM Workshop on Security on Ad Hoc and Sensor Networks, November 3-5, 2004, Washington, DC., USA., pp: 66-67.

Harvard University, 2013. The code blue project, 2013. Harvard University, London. http://www.eecs.harvard.edu/~mdw/proj/codeblue/release/

Josang, A. and R. Ismail, 2002. The beta reputation system. Proceedings of the 15th Bled Electronic Commerce Conference on e-Reality: Constructing the e-Economy, June 17-19, 2002, Bled, Slovenia, pp: 41-55.

Josang, A., R. Ismail and C. Boyd, 2007. A survey of trust and reputation systems for online service provision. Decis. Support Syst., 43: 618-644.

Kamvar, S.D., M. T. Schlosser and H. Garcia-Molina, 2003. The eigentrust algorithm for reputation management in p2p networks. Proceedings of the 12th International Conference on World Wide Web, May 20-24, 2003, Budapest, Hungary, pp: 640-651.

Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1: 293-315.

Karlof, C., N. Sastry and D. Wagner, 2004. TinySec: A link layer security architecture for wireless sensor networks. Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, November 3-5, 2004, Baltimore, MD., USA., pp: 162-175.

Krasniewski, M., P. Varadharajan, B. Rabeler, S. Bagchi and Y.C. Hu, 2005. Tibfit: Trust index based fault tolerance for arbitrary data faults in sensor networks. Proceedings of the International Conference on Dependable Systems and Networks, June 28-July 1, 2005, Los Alamitos, CA., USA., pp: 672-681.

Lawen, A., 2003. Apoptosis-an introduction. Bioessays, 25: 888-896.

Liu, Z., A.W. Joy and R.A. Thompson, 2004. A dynamic trust model for mobile ad hoc networks. Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, May 26-28, 2004, Suzhou, China, pp: 80-85.

Ma, D. and G. Tsudik, 2007. Forward-secure sequential aggregate authentication. Proceedings of the IEEE Symposium on Security and Privacy, May 20-23, 2007, Berkeley, CA., USA., pp: 86-91.

Manzo, M., T. Roosta and S. Sastry, 2005. Time synchronization attacks in sensor networks. Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, November 7-10, 2005, Alexandria, VA., USA., pp: 107-116.

Minder, D., P.J. Marron, A. Lachenmann and K. Rothermel, 2005. Experimental construction of a meeting model for smart office environments. Proceedings of the Workshop on Real-World Wireless Sensor Networks, June 20-21, 2005, Stockholm, Sweden.

Park, T. and K.G. Shin, 2005. Soft tamper-proofing via program integrity verification in wireless sensor networks. IEEE Trans. Mobile Comput., 4: 297-309.

Rebahi, Y., V. Mujica and D. Sisalem, 2005. A reputation-based trust mechanism for ad hoc networks. Proceedings of 10th IEEE Symposium on Computers and Communications, Jun. 27-30, IEEE Xplore, London, pp: 37-42.

Sen, S. and N. Sajja, 2002. Robustness of reputation-based trust: Boolean case. Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems, July 15-19, 2002, Bologna italy, pp: 288-293.

University of Cambridge, 2012. WINES II-smart infrastructure, 2012. University of Cambridge and Imperial College London. http://www.winesinfrastructure.org