Towards Trust-aware Health Monitoring Body Area Sensor Networks

Han Yu[1], Zhiqi Shen[1*], and Cyril Leung[2]

[1]Nanyang Technological University, Singapore (639798)
[2]University of British Columbia, Vancouver, BC V3T 4K1 Canada

yuhan@pmail.ntu.edu.sg, zqshen@ntu.edu.sg, cleung@ece.ubc.ca

Abstract

Background

In many advanced economies of the world, the rising cost of healthcare has become an urgent problem. Wearable networks formed by lightweight sensors and communication devices – body area sensor networks (BASNs) offer a potential way to achieve universal healthcare, but in order to get wide user acceptance, these networks need to be made highly secure and reliable. While traditional cryptographic network security mechanisms can be applied to BASNs to ensure data secure communications, the fact that these networks need to be closely intertwined into social communities, human factors need to be carefully considered to achieve the desired level of reliability. One of the most important human factors for BASNs is the issue of trust. In open environments where these networks may operate in the future, reliability and accuracy may depend on their resistance to dynamic faults or tampering from malicious users.

Method

This paper aspires to take the first look at the possibility of applying trust and reputation management techniques into BASNs. We focus on incorporating trust awareness into beacon based location tracking for body area sensor networks by proposing a novel uncertainty based trust model to improve the effectiveness of an evidence-based trust model against collusion. Extensive computer

* Corresponding author

simulations on three commonly observed types of attacks in such systems have been performed.

Results and Conclusions

The results show that the proposed method is effective in mitigating the adverse effect of malicious nodes in a BASN on the accuracy of location tracking.

Keyword: Trust, Reputation, Body Area Sensor Network, m-Health.

I. Introduction

With the rapid advancement in wireless devices and wireless communications, the e-healthcare industry has moved from the traditional web-based applications where users browse through the relevant information online to learn more about their ailments, to a more ubiquitous setting where sensor devices are attached to the patients who are able to move across a less confined space for medical personnel or caregivers to monitor their physiological conditions or even administer treatments remotely [3], [7], [10], [11], [14]. This citizen-centered approach to healthcare delivery which integrates the use of mobile communication devices is termed Mobile e-Health or m-health for short. Attached or implanted sensor devices on a patient's body form an ultra-small scale network commonly referred to as Body Area Sensor Networks (BASNs) and they provide a cheaper and smarter way to manage and care for patients suffering from chronic illnesses or in the process of rehabilitation. In all these applications, it has been recognized that the problem of location tracking is crucial.

Currently, the Global Positioning System (GPS) is the primary choice for outdoor BASN location tracking where one of the devices attached to a patient is equipped with a GPS receiver which triangulates its location by trying to acquire location signals from at least three satellites and measure the response time. However, in an indoor setting where positioning demands near-instantaneous first-fix and very low power consumption, the present day GPS-based localization method is not a suitable solution [5].

In recent years, beacon based localization techniques [4], [12] have been applied to locating BASNs within large indoor compounds. In these instances, the RF readers or beacon nodes (BNs) are deployed in the target areas in advance. The patients or medical/disaster relief personnel wearing BASN systems carry out their activities in these monitored areas. For beacon based location tracking systems, the BNs only broadcast their own locations and it is the BASNs' responsibility to calculate their own positions and transmit this information back to a central facility.

The environments in which BNs are deployed in may not be secure. Adversaries may capture and compromise one or more BNs or the BNs could suffer failures which may cause them to give out inaccurate location information. In these cases, cryptographic security measures offer little help since the compromised or faulty BNs would have valid credentials. To mitigate the adverse effects of this problem, trust and reputation mechanisms can be very effective [8].

In this paper, we propose a beacon based location tracking system based on trust-aware localization and investigate its effectiveness against BNs which may not only disseminate false location information but may also lie in their testimonies about the behaviors of other BNs. In Section II, the basic system architecture for a beacon-based location tracking system for BASNs is described. In Section III, we will present the detailed trust, credibility and reputation management model that is overlaid on top of the basic location tracking system to provide more secure localization services to the BASNs. Section IV describes the simulations that have been carried out to study the proposed system under different conditions and discusses the results obtained. Section V summarizes the main findings and possible future research directions.

II. Related Work

GPS based positioning is one of the most prevalent means of localization with many areas of application. However, in an indoor environment, GPS based positioning faces grave challenges [5] (e.g. long first-fix time, severe multipath problem, poor accuracy, etc.). Therefore, over the years, beacon-based low cost indoor localization systems have been preferred, especially for very small

devices which cannot accommodate GPS modules in the first place. In [4], a centroid-based location estimation algorithm together with beacon signal acquisition protocols are presented which can achieved a high level of accuracy. The same concept has been applied in [12] to assist BASNs locate themselves in an indoor setting for emergency response. However, these papers do not consider the problem of BNs deployed in an unattended open environment which make them vulnerable to tampering by malicious third parties or malfunctions. In such cases, the use of trust and reputation mechanisms to is often beneficial.

The problem of trust and reputation in beacon based location tracking systems has been studied extensively in the field of wireless sensor networks. Distributed Reputation-based Beacon Trust System (DRBTS) is proposed in [13]. It uses a distributed trust-based security protocol that allows BNs to monitor each other and provide information to sensor nodes (SNs) so that BNs which disseminates false location information can be gradually filtered out. The location estimation method and the protocol for BNs to disseminate their observations about their neighboring BN behaviors assumed in our study are similar to those in DRBTS.

In DRBTS, a BN is assumed to be able to hear the transmissions from all BNs within a one-hop range. It evaluates the validity of the location information communicated by its one-hop neighbors by estimating its own location and comparing the discrepancy to a threshold value. This first-hand observed evidence together with the second-hand evidence shared by other BNs form the reputation belief of a BN on another BN in its neighborhood. Although DRBTS does not specify how the trust evidences are mapped into trustworthiness evaluations for each BN, during the process of aggregating second-hand evidences into the first-hand evidences stored at each BN, a simple deviation test in the form of $\left|R_{j,i} - R_{k,i}\right| < d$ is performed to filter out the potentially unfair evidences from other BNs. The terms $R_{j,i}$ and $R_{k,i}$ are the first-hand evidence from BN_j and BN_k about BN_i respectively and d is a heuristically defined threshold value. DRBTS does not distinguish the trustworthiness of a BN in different contexts. Thus, the behavior of a BN in disseminating location information and its behavior in sharing its testimony about its neighbors' reliability in disseminating

location information are used to update its trustworthiness value. It is then impossible to know if a BN has achieved a high trustworthiness value through good behavior in both of the contexts or just one of them.

In contrast to DRBTS, we distinguished trustworthiness and credibility more systematically. By using an entropy based method to evaluate the degree of uncertainty that can be reduced by incorporating evidences from another BN and separately recording the credibility scores of a BN's neighbors, we provide an interpretation of the deviation test based on information theoretic principles and can improve inference based on past data of which testimonies are more trustworthy. The use of an adaptive forget-factor also makes building reputation harder and losing reputation easier.

III. Network Architecture

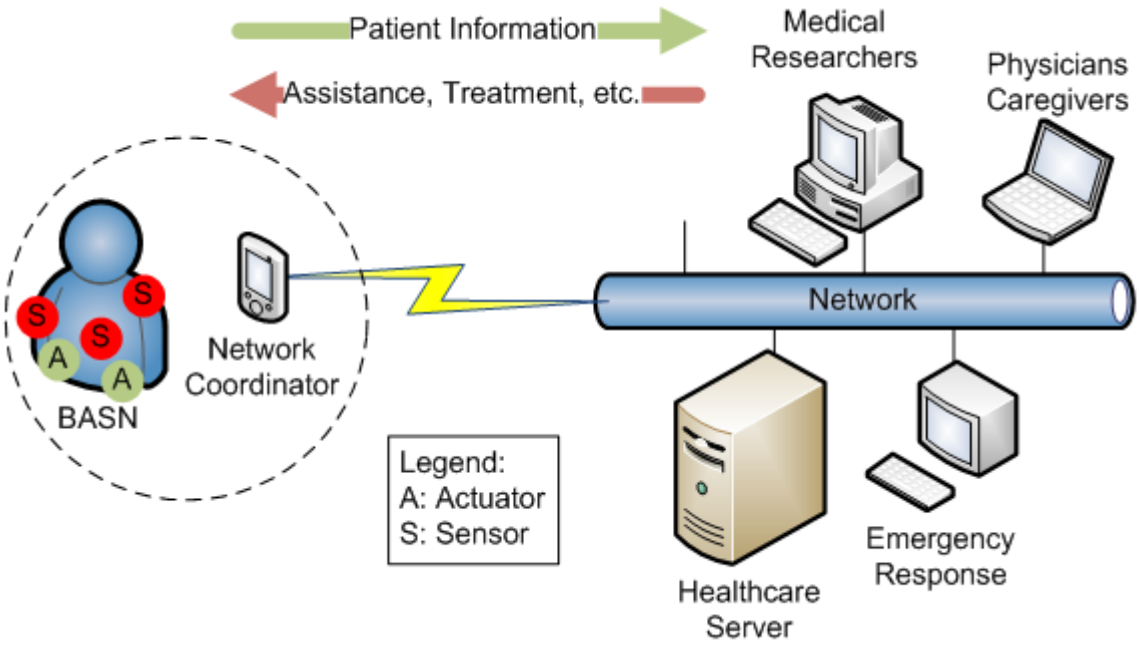

Figure 1. The network architecture of a typical health monitoring BASN.

A BASN, depending on the field of application, normally consists of a set of low power, non-intrusive sensor/actuator devices each monitoring/controlling a specific aspect of the human body (e.g. physiology or bio-kinetics) that are either attached to or implanted into the patient [1]. Due to

size and weight limitations, these devices generally have very modest computational and communications power. Therefore, a mobile device such as a personal digital assistant (PDA) usually acts as a network coordinator to transmit the sensing results to and instructions from the healthcare servers as illustrated in Figure 1. The actuators are optional depending on whether the BASN is designed to provide remote and immediate aid to the patient.

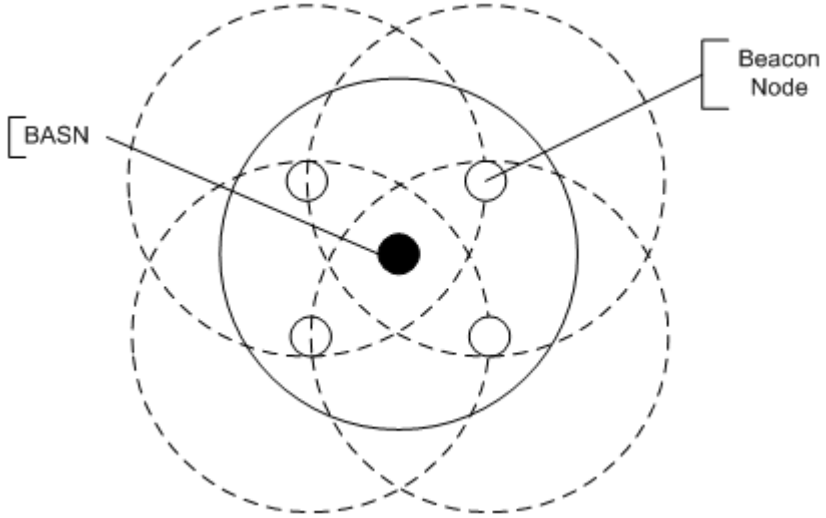

Figure 2. The beacon-based location tracking technique for BASNs.

The network coordinators are also responsible for determining the locations of the BASNs and relay this in-formation to the central facility for medical staff or emergency response commanders to keep track of the patients. In a typical beacon-based location tracking system for sensor networks, the responsibility for localization lies with the receiver nodes (sensor nodes) that needs to be localized [4]. This is to ensure that the system scales well to large distributed networks in which there are many receivers whose positions need to be tracked.

In this paper, we consider a network of N BNs b_1, b_2,… , b_N that have been deployed to a medical complex or residential/commercial building to form a regular mesh as shown in Figure 2. The dashed circular lines indicate the transmission range of the BNs while the solid circular line indicates the transmission range of a BASN. The following assumptions are made:

1) Once deployed, the BNs remain stationary.

2) A BN multicasts its location information when it receives a request.

3) Since the responsibility of determining the location of a BASN lies with the network coordinator of that BASN, the BNs only transmit their own location in-formation to the requesting BASNs.
4) Since multiple organizations may be involved, it could be difficult to implement pair-wise encryption key between the BASNs and the BNs. Therefore, we assume the encryption of the location information is achieved by using a network-wide key that enables other BNs within transmission range to hear the broadcast from any particular BN.

The BNs have identical idealized spherical radio transmission range.

IV. Trust and Reputation Management

The Basic Trust Evaluation Model

In order to filter out malicious or faulty BNs during the localization process, we propose a trust management system which uses the concept of reputation, trust and credibility in conjunction with the basic beacon based location tracking system described in the previous section. According to [9]: "reputation is what is generally said or believed about a person's or thing's character or standing". In our case, it is what a group of neighboring BNs which can hear *BNi* generally believes about the correctness of the location data transmitted by *BNi*. The reputation evaluation is important for the requesting BASN to determine which BNs are to be trusted when attempting to locate itself. In order to form the reputation belief, the trust beliefs from each individual BN in the group need to be aggregated. We adapt the view on reliability trust from [9] to consider trust here as the subjective probability held by an individual that another individual will perform a given action correctly. When *BN1* overhears the transmitted location information from *BN2* in response to a request from a BASN, it estimates its own location based on the claimed location of *BN2* [13]. If the result is within a tolerable margin of error, the location data provided by BN2 is regarded as correct and *BN1*'s trust in BN2

increases. Otherwise, *BN2* is considered potentially malicious and *BN1*'s trust in *BN2* is decreased.

Since the only action a BN performs in the basic system model is to broadcast its own location coordinates, it is possible for it to lie about its own location only. Thus, the trust model needs to deal with only one context – the trustworthiness of BNs when reporting their own locations. However, as a BASN moves around the monitored area, the group of BNs that can respond to its localization requests is determined by the actual location of the BASN and the BN transmission range. This dynamic nature of BN group formation makes it very difficult to set up in advance group leaders which can store the reputations of all the group members. Therefore, we adopt a distributed trust model based on past experiences where each BN stores its past direct interaction experiences (i.e. the number of correct and incorrect location broadcasts from each neighboring BN) locally. The outcome of each reporting is considered either completely correct (as long as the location coordinates are within a predetermined range of precision) or completely wrong. The experience history can be recorded as a vector $R(t) = \begin{bmatrix} r \\ s \end{bmatrix}$ where *R(t)* is a first-hand evidence of a BN's behavior at time instance *t* and *r* and *s* denote correct and incorrect report respectively; *r* and *s* can be either 0 or 1. The Beta Reputation Model [9] can then be used to derive the trustworthiness score of a BN in the view of another BN. The aggregated total past behavior of a BN as observed by another BN is recorded as:

$$\boldsymbol{R_{total}(t) = \rho R_{total}(t-1) + (1-\rho)R(t)} \quad (1)$$

where $\rho \in [0,1]$ is a forget-factor. It controls the relative importance given to the latest observation and the past observations. After combining the latest observation, $R_{total}(t)$ is in the form of $\{\begin{bmatrix} p \\ n \end{bmatrix} | p, n \in R^+\}$. From this evidence, the Beta Reputation Model derives the trustworthiness of a BN from the perspective of another BN as $\tau = \frac{p+1}{p+n+2}$. A τ value near 0 indicates low trustworthiness whereas $\tau \approx 1$ indicates high trustworthiness. In order to

incorporate the intuition that the reputation of a BN should be easy to lose but hard to build, we let the forget-factor vary according to the latest observed behavior in the following manner:

$$\boldsymbol{\rho} = \begin{cases} \boldsymbol{\rho_0}, \ \boldsymbol{if\ R(t)} = \begin{bmatrix} \mathbf{1} \\ \mathbf{0} \end{bmatrix} \\ \mathbf{1} - \boldsymbol{\rho_0}, \ \boldsymbol{if\ R(t)} = \begin{bmatrix} \mathbf{0} \\ \mathbf{1} \end{bmatrix} \end{cases} \tag{2}$$

where ρ_0 is a value close to 1. A general guideline for the value of ρ_0 given in [2] is that $\rho_0 = 1 - \frac{1}{m}$, where m is the number of observations over which a BN behavior does not change significantly. The use of (2) implies that an observation of a bad behavior of a BN has a greater effect on its reputation than an observation of good behaviors.

An Entropy-based Credibility Evaluation Model

To a BASN which is requesting localization assistance, the reputation of a BN is a good measure on how much confidence can be placed on its location report. Intuitively, the BNs should send their own observed past evidence (hereafter referred to as *testimonies*) about their neighboring BNs to the BASN for it to make a reputation evaluation. However, testimony sharing opens up a new avenue for BNs to misbehave and there is no definitive way to ascertain the truthfulness of the testimonies. As the BASN does not know its most up-to-date location, it is difficult for it to know if the location information from any BN is correct or not. On the other hand, the BNs are assumed to have the capability to evaluate whether the location information it overhears from another BN indeed reflects the true position of that BN. Therefore, in our proposed trust management model, the responsibility for forming reputation beliefs rests with the BNs in the neighborhood. The BNs need to disseminate their testimonies within their neighborhood. Each BN then combines the received testimonies with its own first-hand evidences to form its view of the reputations of its neighbors.

Since the trustworthiness (and hence reputation) of a BN is only updated by its neighbors when it broadcasts its location information upon request from BASNs, in our trust management model, the BNs broadcast their testimonies (i.e. $R_{total}(t)$) together with their own location information. Other BNs within radio range of a transmitting BN then subject these testimonies to the entropy based deviation test in [15] to determine how much the received evidence differs from the current belief.

The entropy of a discrete random variable V is calculated as [6]:

$$\boldsymbol{H(V) = -\sum_i \Pr(v_i) \log(\Pr(v_i))} \quad (3)$$

where v_i is a possible value of V and $Pr(v_i)$ is the probability of V taking on value of v_i. The entropy is a common measurement of information uncertainty. In our case where the trust evidence takes on binary values, the entropy can be calculated as:

$$\boldsymbol{H(R_{total}(t)) = -\Pr(p) \log(\Pr(p)) - \Pr(n) \log(\Pr(n))} \quad (4)$$

where $\Pr(p) = \frac{p+1}{p+n+2}$ and $\Pr(n) = \frac{n+1}{p+n+2}$. The *quality* of the testimony is measured according to the uncertainty it contains as follows:

$$\boldsymbol{Q(R) = \frac{H_{max} - H(R)}{H_{max} - H_{min}}} \quad (5)$$

where $Q(R)$ represents the quality of the current belief with testimony R incorporated. In the case of binary ratings, H_{max} occurs when $\Pr(p) = \Pr(n)$, i.e. the number of positive and negative observations are equal, whereas H_{min} occurs when either p or n completely dominates the other. The quality, $Q(R_M)$, of a BN's current belief on another BN is initialized using only its first-hand evidences on that BN. After that, each testimony is subjected to a deviation test as follows:

$$\boldsymbol{|Q(R) - Q(R_M)| \leq \varepsilon} \quad (6)$$

where $\varepsilon \in [0,1]$ is the filtering threshold which controls the sensitivity to the presence of unfair testimonies: the smaller the value of ε, the more sensitive the truster BN is to unfair testimonies. If the testimony passes the deviation test, it is aggregated into the current belief

and $Q(R_M)$ is updated. To distinguish between the concept of trust in our model which is used to evaluate the behaviors of BNs in the context of reporting their location information, we uses the term *credibility* to describe the trustworthiness of a BN in the context of sharing testimonies. The credibility evidences are recorded in the same way as trust evidences and it is also evaluated using the formulae from the Beta Reputation Model. Therefore, if a testimony passes the deviation test, its credibility will be increased. In the case where a testimony fails a deviation test, the BN will first look at the previous credibility evidences to estimate the credibility of the referrer BN. If its credibility exceeds a predefined threshold value, it is likely that the behavior of the target BN in terms of reporting its own location information has drastically changed and the testimony will be aggregated into the current belief. Otherwise, the testimony will be rejected and the credibility of the referrer BN will be reduced. The aggregation is accomplished by using the formula:

$$\boldsymbol{R_{total}(t) = wR_{total}(t-1) + (1-w)cR_r(t)} \quad (7)$$

where $w \in [0,1]$ is a weight given to the current belief which need to be heuristically determined by the system designer, $c \in [0,1]$ is the credibility of the referrer BN and $R_r(t)$ is the trust evidence shared by the referrer BN on another target BN. After the new evidences are incorporated into the current belief, the $Q(R_M)$ is updated and the procedure carries on until all the received testimonies are processed.

Evaluating Reputation

The reputation of all the neighboring BNs of any BN is the trustworthiness value derived from the aggregated trust evidences on those BNs. Each BN stores the list of reputation values of its neighbors locally. When a BASN requests for localization assistance, the BNs broadcast three items:

1) Its location information (i.e. ID and location coordinates);

2) The list of reputation values of its neighbors (i.e. within one-hop transmission range) from the last update;

3) Its first-hand trust evidences for all its neighbors.

The first and second items are for the BASNs to use to location themselves while the first and third items are for other BNs to update their reputation, trust and credibility evidences. Once the BASN receives the location information and reputation lists from BNs within its own one-hop transmission range, it will first estimate the overall reputation of each BN as follows:

$$\mathbf{r_i} = \frac{\mathbf{1}}{\mathbf{k}} \sum_{\mathbf{j=1}}^{\mathbf{k}} \mathbf{r_{ij}} \tag{8}$$

where r_i is the reputation of BN_i, k is the total number of reputation lists containing the reputation value for BN_i received, and r_{ij} is the reputation of BN_i as in reputation list j. If r_i exceeds a predefined threshold for reputation requirement (an intuitive value could be 0.5 when r_i takes a value from 0 to 1), the location information from BN_i will be used to estimate the current location of the BASN; otherwise, its location information will be discarded. This method of filtering off potentially incorrect location information from the BNs is essentially a quorum voting approach. Thus, it should be effective only under the condition that the majority of the BNs are benign and not faulty.

V. Empirical Evaluation

Empirical studies have been carried out in the form of software simulations in a Java based test-bed we have developed. The BNs in the simulation are assumed to be arranged in a regular mesh where every BN has a number of other BNs located within its one-hop range depending on the configuration of the building. All BNs are assumed to have the same one-hop communication range. BASNs are initially randomly placed into the mesh and they move through the mesh in discrete time steps in randomly generated directions.

In our experiments, we investigated the attack scenarios where BNs can lie about both their locations as well as their reputation evaluation on their neighboring BNs. We focus our discussions here on three types of commonly studied methods of attack – on-off attack, badmouthing and ballot stuffing.

The metrics that are monitored during the experiments are Mean Square Error (MSE) of the estimated distance and Misdetection Rate *m*. The MSE is calculated as:

$$MSE = \frac{1}{k}\sum_{i=1}^{k} \sqrt[2]{(X_{est} - X_i)^2 + (Y_{est} - Y_i)^2} \quad (9)$$

where X and Y are the actual location coordinates of a BASN and X_{est} and Y_{est} are the estimated location coordinates of that BASN and k is the total number of malicious BNs engaging in the specific attack in the network. The smaller the MSE value is, the more accurate a method is in locating a BASN in a beacon network and vice versa.

A. On-off Attack

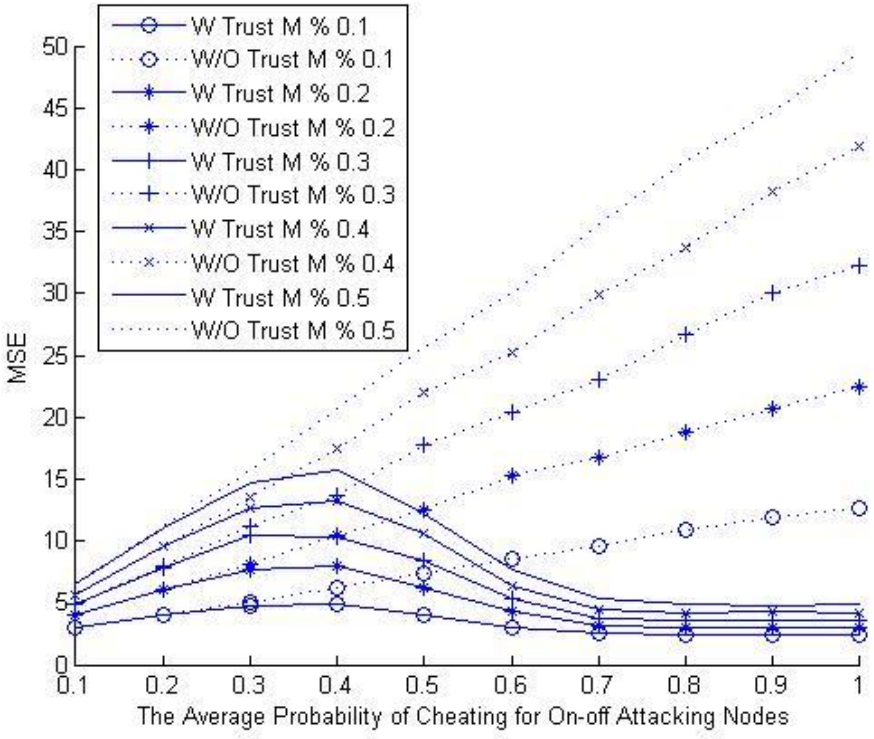

Figure 3. The average MSE of the BASNs against the average probability of Cheating for BNs engaging in the On-off Attack.

BNs with static behaviors (e.g. always lying about their locations or always broadcasting correct location information) are relatively easier to be identified by most trust models. However, those which alternate between periods of accurate location reporting and periods of disseminating incorrect information are harder to detect. This type of attack on the trust management system is known as the on-off attack. In our experiments, we investigated the on-

off attack scenarios where BNs can lie about their locations. We assume that all malicious BNs engaging in the on-off Attack has the same probability of lying. Two parameters are varied to observe the performance of the proposed trust management system: *P1* is the percentage of malicious BNs in the entire BN network lying about their locations; *Pr1* is the probability a BN giving out false location information. *P1* is limited to the range of 0 to 50%. The reason is that our proposed system relies on a modified majority voting mechanism to detect the malicious nodes and, therefore, it assumes that the majority of BNs are benign. *Pr1* is varied from 0 to 100%, whereas 0% acts as the best case scenario where none of the malicious BNs ever lies and 100% acts as the worst case scenario where malicious BNs lie all the time about their locations. In these experiments, it is assumed that the reputation information on a BN shared by all the BNs is not tampered with.

As can be observed from Figure 3, for a fixed proportion of on-off attackers in a beacon network, the MSE value improves with the average probability of cheating for the on-off attacking nodes. This is because with low probability of cheating, a malicious node's reputation might not be reduced to a level low enough to classify it as malicious. As the average probability of cheating increases, in all network configurations with differing proportions of malicious nodes, the system with the proposed trust model significantly outperforms that without it.

B. Ballot-stuffing Attack

Ballot-stuffing is a type of attack where the attacking BNs deliberately alter their reputation evaluation for BNs that give out incorrect location information to make them appear highly trustworthy. In our experiments, this is accomplished by making the attacking BNs broadcast the number of incorrect location reporting of other malicious BNs as the number of correct location reporting and vice versa. To isolate the effect of ballot-stuffing attackers, we assumed that the malicious BNs lie about their locations with a probability of 0.5. We then alter *P2* (the percentage of BNs engaging in ballot-stuffing attack in the BN network) between 0 and 50% to

observe the effectiveness of the proposed trust model. *Pr2* is fixed at the value of 100%. The average MSE is monitored to evaluate the performance of the proposed trust management system.

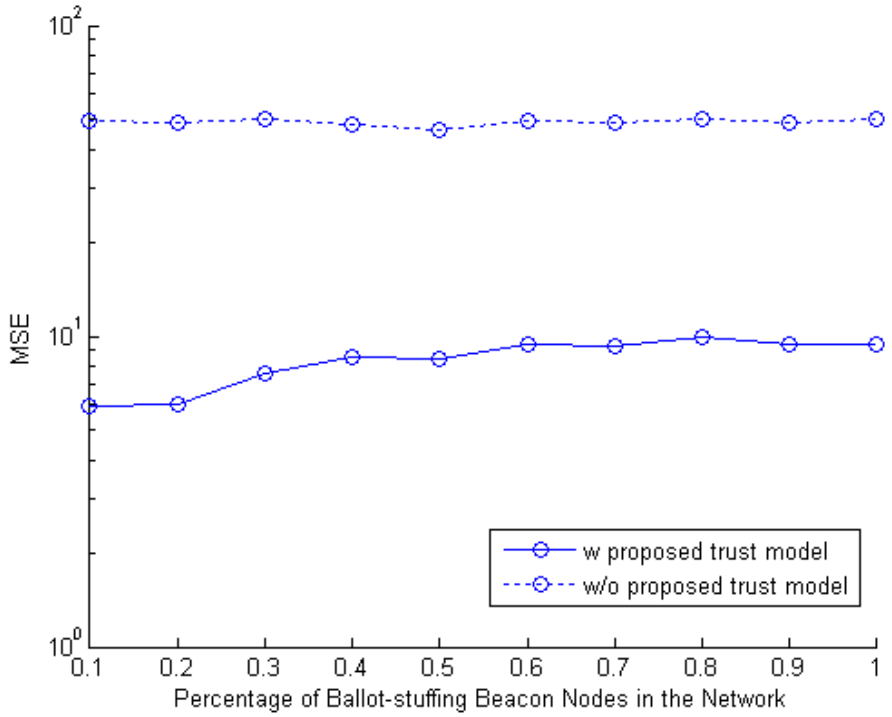

Figure 4. The average MSE of the BASNs against the percentage of Ballot-stuffing BNs in a network.

As shown in Figure 4, the MSE of the system with the proposed trust model consistently outperforms that with only the basic trust model illustrated in Section IV.A With ballot-stuffing attack, some BNs which rarely provide correct location information might be rated highly in the trustworthiness scale due to unfairly inflated testimonies, which could result in the location information reported by them being given highly skewed weight. This effect, if unchecked, could severely mislead the BNs into giving higher weight to incorrect information and lead to larger positioning errors.

When the percentage of ballot-stuffing BNs in the network is high, the MSE of the system with the proposed trust model rise to higher levels indicating a degradation in the system performance. In this case, after the filtering operation, only the opinion of very few BNs might

be left to form a reputation evaluation. Thus, the BNs have to trust less on the opinion shared by their neighboring BNs on the reliability of the location information provided by any BN in the network. More risks have to be taken by every individual BN in order for them to form a belief on the trustworthiness of others. Therefore, with the increase in the exposure to potentially malicious BNs, the error in the location information supplied to the requesting BASNs increases during the experiments. With the proposed trust model, the impact of both the malicious BNs as well as the ballot-stuffing BNs on the correctness of the location information provided is drastically reduced.

C. Badmouthing Attack

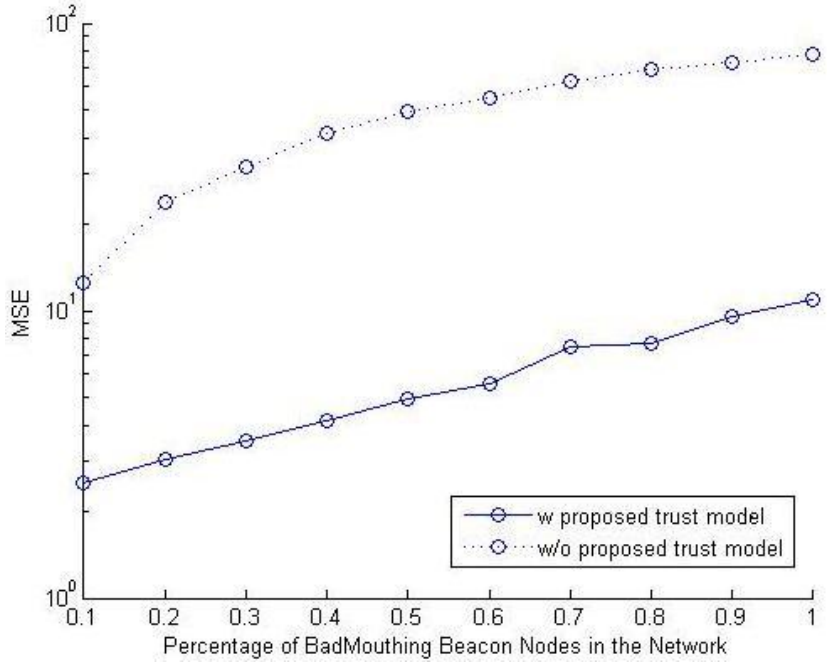

Figure 5. The average MSE of the BASNs against the percentage of Badmouthing BNs in a network.

Bad-mouthing is a type of attack where the attacking BNs deliberately alter their reputation evaluations on non-malicious BNs to make them appear less trustworthy. In our experiments, this is accomplished by making the attacking BNs broadcast the number of incorrect location reporting of the non-malicious BNs as the number of correct location reporting and vice versa. To isolate the effect of bad-mouthing attackers, we assumed that the malicious BNs lie about

their locations with a probability of 0.5. We then alter *P3* (the percentage of BNs engaging in bad-mouthing attack in the BN network) between 0 and 50% to observe the effectiveness of the proposed trust model. *Pr3* is fixed at the value of 100%. The average MSE is monitored to evaluate the performance of the proposed trust management system.

Badmouthing has the opposite effect from ballot-stuffing. In this case, malicious node's reputation does not get a boost, but the reputation of trustworthy beacon nodes is reduced by the badmouthing report. If the reputation reports of the badmouthing BNs are not filtered out, the BASNs in the network may have difficulty acquiring location information from enough trusted BNs (i.e. BNs with reputation above certain threshold) to make an accurate estimation of its current location. From Figure 5, it can be observed that the MSE of the system with the proposed trust model consistently outperforms that with only the basic trust model illustrated in Section IV.A.

VI. Conclusions

In this paper, we advocate the importance of trust and reputation management in BASNs and adapted a novel uncertainty based testimony filtering method to propose a trust management system which provides trust aware location tracking service to BASNs in a beacon based location system. With this service, BASNs can greatly improve the reliability of location estimation for remote medical assistance or emergency response systems in possibly hostile environments. Preliminary computer simulation studies have confirmed the viability and effectiveness of the proposed system.

In order to employ the system in a practical network, further improvements and studies are needed. For this purpose, we aim to develop a realistic software test-bed to provide the researchers with a fast and low cost way to check the effectiveness of their proposed trust model. New mechanisms for neighborhood monitoring and reputation information propagation will be refined with the aim to reduce communication overhead. The possibility of applying lower communications overhead

versions of the proposed trust model to networks with even lower bandwidth resources such as the radio frequency identification (RFID) based networks will also be explored.

Acknowledgement

This research is supported, in part, by the Singapore Millennium Foundation (SMF).

References

[1] BIELSKIS, A.A., DENISOVAS, V., DRUNGILAS, D., GRICIUS, G. AND RAMAŠAUSKAS O. 2008. Modelling of Intelligent Multi-Agent based E-health Care System for People with Movement Disabilities. *Elektronika Ir Elektrotecknika*, 2008. 6(86).

[2] BUCHEGGER, S. AND BOUDEC, J.-Y.L. 2004. A Robust Reputation System for P2P and Mobile Ad-hoc Networks. In *Proceedings of the 2nd Workshop on the Economics of Peer-to-Peer Systems*. Cambridge MA, USA.

[3] BULTS, R., WAC, K., HALTEREN, A.V., KONSTANTAS, D., JONES, V. AND WIDYA, I. 2004. Body Area Networks for Ambulant Patient Monitoring Over Next Generation Public Wireless Networks. In *3rd IST Mobile and Wireless Communications Summit*.

[4] BULUSU, N., HEIDEMANN, J. AND ESTRIN, D. 2000, GPS-less Low Cost Outdoor Localization for Very Small Devices. *IEEE Personal Communications Magazine*, 28-34.

[5] DEDES, G. AND DEMPSTER, A.G. 2005. Indoor GPS Positioning - Challenges and Opportunities. In *62nd IEEE Vehicular Technology Conference (VTC)*, Vol. 1, 412- 415.

[6] GALLAGER, R.G. 1968. Information Theory and Reliable Communications, *J. Wiley*, 588.

[7] HANSON, M.A., POWELL, H.C. Jr., BARTH, A.T., RINGGENBERG, K., CALHOUM, B.H., AYLOR, J.H. AND LACH, J. 2009. Body Area Sensor Networks: Challenges and Opportunities. *Computer*, 42(1), 58-65.

[8] HEUWINKEL, K. AND DEITERS, W. 2003. Information Logistics, E-healthcare and Trust. In *IADIS International Conference e-Society*.

[9] JØSANG, A., ISMAIL, R. AND BOYD, C. 2007. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 43(2), 26.

[10] JOVANOV, E. 2005. Wireless Technology and System Integration in Body Area Networks for m-Health Applications. In *27th Annual International Conference of the Engineering in Medicine and Biology Society, IEEE-EMBS*, 17-18.

[11] JOVANOV, E., MILENKOVIC, A., OTTO, C. AND GROEN, P.C.d. 2005. A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation. *Journal of Neuro Engineering and Rehabilitation*, 2(6).

[12] LORINCZ, K., MALAN, D.J., FULFORD-JONES, T.R.F., NAWOJ, A., CLAVEL, A., SHNAYDER, V., MAINLAND, G. AND WELSH, M. 2004. Sensor Networks for Emergency Response: Challenges and Opportunities. *IEEE Pervasive Computing*, 3(4), 16-23.

[13] SRINIVASAN, A., TEITELBAUM, J. AND WU, J. 2006. DRBTS: Distributed Reputation-based Beacon Trust System. In *Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC 06)*, Washington D.C., USA. 277-283.

[14] WANG, Y. AND SINGH, M.P. 2007. Formal Trust Model for Multiagent Systems. In *20th International Joint Conference on Artificial Intelligence (IJCAI)*.

[15] WENG, J., MIAO, C. AND GOH, A. 2006. An Entropy-based Approach to Protecting Rating Systems from Unfair Testimonies. *IEICE - Transactions on Information and Systems*, E89-D (9).

Han Yu received the B.Eng. degree in computer engineering from Nanyang Technological University (NTU), Singapore, in 2007, where he is currently working towards the Ph.D. degree at the School of Computer Engineering.

He is a Singapore Millennium Foundation (SMF) Ph.D. scholar. He worked as a Systems Engineer in Hewlett-Packard Singapore Pte. Ltd. from 2007 to 2008. His research interests include trust management in multiagent systems and intelligent agent augmented interactive digital media in education.

Zhiqi Shen received the B.Sc. degree in computer science and technology from Peking University, Beijing, China, the M.Eng. degree in computer engineering from Beijing University of Technology, Beijing, China, and the Ph.D. degree from the Nanyang Technological University, Singapore.

Currently, he is with the Division of Information Engineering, School of Electrical and Electronic Engineering, Nanyang Technological University. His research interests include artificial intelligence, software agents, multiagent systems (MAS); goal-oriented modeling, agent-oriented software engineering; semantic web/grid, e-learning, bioinformatics and biomanufacturing; and agent-augmented interactive media, game design, and interactive storytelling.

Cyril Leung received the B.Sc. degree (honors) from Imperial College, University of London, London, U.K., in 1973 and the M.S. and Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, in 1974 and 1976, respectively.

From 1976 to 1979, he was an Assistant Professor at the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge. During 1979–1980, he was with the Department of Systems Engineering and Computing Science, Carleton University, Ottawa, ON, Canada. Since July 1980, he has been with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada, where he is a Professor and currently holds the PMC-Sierra Professorship in Networking and Communications. His current research interests are in wireless communications systems.

Dr. Leung is a member of the Association of Professional Engineers and Geoscientists of British Columbia, Canada.