Computers in Human Behavior xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Secure transfer of environmental data to enhance human decision accuracy

Kashif Saleem [a,*], Abdelouahid Derhab [a], Jalal Al-Muhtadi [b], Basit Shahzad [c], Mehmet A. Orgun [d]

[a] Center of Excellence in Information Assurance (CoEIA), King Saud University (KSU), Riyadh, Saudi Arabia
[b] Center of Excellence in Information Assurance (CoEIA), College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia
[c] College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia
[d] Intelligent Systems Group (ISG), Department of Computing, Macquarie University, NSW 2109, Australia

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Accuracy
Blood brain barrier
Communication
Irrigation
Security
Wireless Sensor Network

ABSTRACT

A critical issue in environmental decision making is how to trust the monitoring information gathered by a multitude of devices at remote locations. The accuracy of information helps in enhancing the effectiveness of decisions, whether it is made by human beings or by an intelligent system. The researchers and practitioners from disciplines such as climatology, agriculture, and meteorology, which depend on the environmental data, are heavily affected in the case of inaccurate information. In order to deal with the above problem, in this paper a data encryption algorithm inspired by the blood brain barrier (BBB) system. A real scenario to irrigate a remote location based on a wireless sensor network (WSN) is simulated in network simulator 2 (ns-2) to study the performance of the encryption algorithm. Our result and analysis show that the proposed encryption mechanism can efficiently protect the data communication from brute-force search or exhaustive key search, eavesdropping, spoofed, altered or replayed routing information, selective forwarding, acknowledgement spoofing, sybil and hello flood attacks. Hence, the proposed data encryption algorithm ensures the confidentiality of critical information from source to a given destination, which ultimately helps in enhancing the human decision accuracy and learning environmental conditions.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

The modern daily life depends on the execution of many complex tasks that vary due to situations, scenarios and time constraints, whereby some tasks depend on others and some need to be performed in parallel. Multi-tasking in such scenarios is very challenging to most human beings, resulting in mishandled and/or incomplete tasks (Adler & Benbunan-Fich, 2013), especially in older ages (Barnard, Bradley, Hodgson, & Lloyd, 2013). Therefore, to manage the tasks of the modern daily life despite their complexity, human beings need assistance (Low & Beukelman, 1988). The assistance can be provided by distributing the tasks to other human beings, which in turn generates privacy issues, or by delegating some of the tasks to intelligent devices for assistance (Rizzuto, 2011; Shahzad & Afzal, 2007; Shahzad & Safvi, 2010; Wagner, Hassanein, & Head, 2010). Smart intelligent devices can perform their allocated tasks actually faster and more accurately (Klein, Nir-Gal, & Darom, 2000; Lucas, Gratch, King, & Morency, 2014; Madhavan & Phillips, 2010) like the human being speaks or dictates and the smart devices take exact actions accordingly (Yeh, Pao, Lin, Tsai, & Chen, 2011) and/or computer speaks and assists human beings in behavior enhancement (Bailey, Adamczyk, Chang, & Chilson, 2006; Lundberg & Olofsson, 1993).

One of the most critical and important environmental scenarios all around the world is to control the wastage of fresh water and optimize systems for better consumption (Alexandratos & Bruinsma, 2012). It is acknowledged that 1.1 billion people across the world live without satisfactory access to clean water. Quite remarkably, and despite growing water scarcity creating a need to be more efficient, one can observe an overall ill-adapted use of resources, especially in the primary sector. Today, the standard irrigation method (Montanabw., 2010) consumes 70% of the fresh water used worldwide by human activity (Alexandratos & Bruinsma, 2012; Kijne, 2003). More generally, it is estimated that 40% of the fresh-water used for agriculture in developing countries is lost, be it by evaporation, spills, or absorption by the deeper layers of the soil, beyond the reach of plants' roots (Alexandratos &

* Corresponding author.
E-mail addresses: ksaleem@ksu.edu.sa (K. Saleem), abderhab@ksu.edu.sa (A. Derhab), jalal@ccis.edu.sa (J. Al-Muhtadi), basit.shahzad@gmail.com (B. Shahzad), mehmet@science.mq.edu.au (M.A. Orgun).

http://dx.doi.org/10.1016/j.chb.2015.01.023
0747-5632/© 2015 Elsevier Ltd. All rights reserved.

Bruinsma, 2012). Consequently, immediate water-related agricultural concerns have become important on the agenda of the governments of arid and semi-arid regions of the world. Indeed, a rational agricultural water management becomes compulsory, and many related issues are waiting for solutions from the scientific and industry communities.

Proper timing of irrigation and amount of water to apply are two crucial decisions for a farmer to: (1) meet the water needs of the crop to prevent yield loss due to water stress, and (2) minimize water wastage. This is achieved by adopting different irrigation scheduling methods, which range from simple calendars to high-technology methods.

Precise irrigation is only possible with regular monitoring of the soil water and crop development conditions in the field. The recent emergence of wireless sensor networks (WSNs) has allowed the implementation of low-cost and real-time monitoring systems for the agricultural fields. Wireless sensor networks are a network of tiny and low-cost sensor nodes designed to gather environmental data using sensing capabilities and transfer them to the destination known as the sink node (or the base station). WSNs are ideal for applications in remote places with very limited infrastructure because they are low cost, fast to deploy, and easy to maintain. Furthermore, sensor nodes work in a self-organized manner to perform the required tasks and take the irrigation decisions (Yunseop, Evans, & Iversen, 2008). These features have the potential to maximize the automated tasks, which reduce the workload of the farmers.

Fig. 1 shows a scenario of a WSN-based irrigation system. In the figure, a wireless sensor mote periodically monitors and collects the required agricultural parameters (i.e., soil moisture, temperature, humidity) related to a given region. Then it sends the collected data to the base station using a routing protocol. The decision and visualization center at the base station decides whether it is necessary to perform the irrigation and for how long. The decision considers the information collected from the sensor motes, the soil model and the crop model. Then, the base station notifies the farmer through email or SMS, about the irrigation decision. The farmer in this case, can remotely, via a web application or on a mobile device, send instructions to open or close the valve.

In the recent literature, while routing strategies and WSN modeling have been getting much attention, security issues have not received extensive focus (Saleem, Fisal, & Al-Muhtadi, 2014). In WSNs, many routing protocols are very simple, and for this reason, WSNs are prone to diverse attacks. In a WSN, an adversary can either deploy his own node or compromise some other nodes. The compromised nodes can take many actions to create network layer attacks depending on the manipulated sensor data. The attacks can be divided into two classes: (1) those that try to manipulate the user data directly and (2) those that try to affect the underlying data routing topology. In the context of irrigation, some attacks might compromise the irrigation decisions to cause over-irrigation or the application of water which is less than the required amount. This can occur, for instance, by injecting false information in the network or by compromising the sensor node controlling the valve.

It is imperative that the security concerns be addressed from the beginning of the design of WSN (Walters & Liang, 2007) so that the farmer can trust the irrigation decisions made and adopt the WSNs for irrigation scheduling. Because of resource limitations and vulnerabilities of wireless communication, WSNs may suffer from a multitude of attacks, if the wireless sensor nodes are deployed in an environment that is unprotected/hostile (Karlof & Wagner, 2003; Pathan, Lee, & Hong, 2006; Xiangqian, Makki, Kang, & Pissinou, 2009). There have been many proposals for routing in WSNs deployed in such often hostile and unpredictable environments. For instance, one of the recently proposed routing protocols (Saleem et al., 2014) requires active as well as efficient security measures. This is because such a protocol requires certain time to develop overall network knowledge at the initialization phase after deployment. The initialization phase is critical in the complete life span of WSNs. When the nodes are deployed, they have to acquire and build the neighboring and environmental information to communicate and transfer data to the required destination effectively.

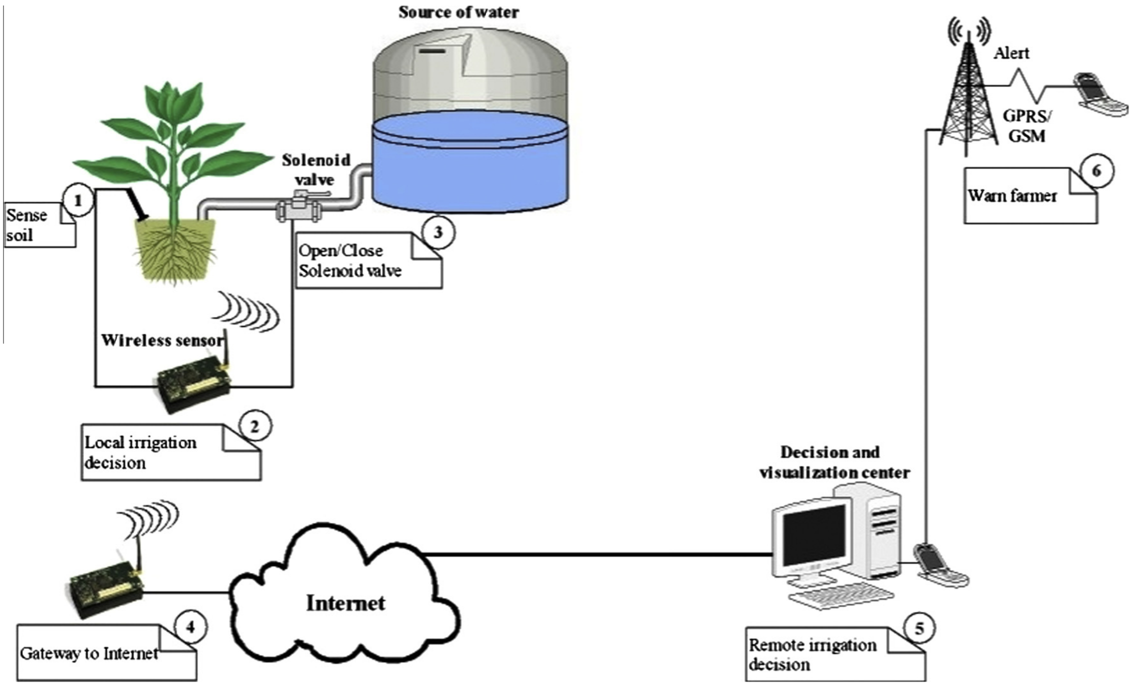

Fig. 1. Real WSN based irrigation scenario.

Download English Version:

https://daneshyari.com/en/article/10312602

Download Persian Version:

https://daneshyari.com/article/10312602

Daneshyari.com