Ad Hoc Networks 13 (2014) 94–106

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

Dependable wireless sensor networks for reliable and secure humanitarian relief applications

Issa M. Khalil [a,*], Abdallah Khreishah [b], Faheem Ahmed [a], Khaled Shuaib [a]

[a] College of Information Technology, United Arab Emirates University, United Arab Emirates
[b] Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, United States

ARTICLE INFO

Article history:
Received 29 October 2011
Received in revised form 12 June 2012
Accepted 17 June 2012
Available online 23 June 2012

Keywords:
Local monitoring
Identity delegation
Multi-hop wireless networks
Packet dropping
Security attacks

ABSTRACT

Disasters such as flooding, earthquake, famine and terrorist attacks might occur any time anywhere without prior warnings. In most cases it is difficult to predict when a disaster might occur however, well-planned disaster recovery procedures will reduce the intensity of expected consequences. When a disaster occurs, infrastructure based communications are most likely to be crippled, worsening the critical situation on hand. Wireless ad hoc and sensor network (WASN) technologies are proven to be valuable in coordinating and managing rescue operations during disasters. However, the increasing reliance on WASNs make them attractive to malicious attackers, especially terrorist groups, in a bid to hamper rescue operations amplifying the damage and increasing the number of casualties. Therefore, it is necessary to ensure the fidelity of data traffic through WASN against malicious traffic disruption attacks. In this paper, we first demonstrate how WASN can be used in a well-planned disaster recovery effort. Then, we introduce and analyze one of the most severe traffic disruption attacks against WASNs, called *Identity Delegation*, and its countermeasures. Its severity lies in its capability to evade detection by even state-of-the-art intrusion detection techniques such as the neighbor monitoring based mechanisms. Through identity delegation, an adversary can drop packets, evade detection, and frame innocent nodes for dropping the traffic. We introduce a technique to mitigate identity delegation attack, dubbed SADEC, and compare it with the state-of-the-art mitigation technique namely Basic Local Monitoring (BLM) under a wide range of network scenarios. Our analysis which is validated by extensive ns-2 simulation scenarios show that BLM fails to efficiently mitigate packet drop through identity delegation attacks while SADEC successfully mitigates them. The results also show that SADEC achieves higher delivery ratios of data packets compared to BLM. On the other hand, the results show similar behavior in framing probabilities between SADEC and BLM. However, the desirable features of SADEC come at the expense of higher false isolation probabilities in networks with heavy traffic load and poor communication links.

1. Introduction and related work

Several applications have been envisioned for Wireless Ad hoc and Sensor Networks (WASNs) [18–20]. In addition to many applications in the military domain, WASNs have seen increased applications in the civilian domain including habitat monitoring, animal tracking, forest-fire detection [20], disaster relief and rescue, oil industry management, traffic control and monitoring, etc. Disaster relief and human rescue applications are receiving growing attentions as disasters, man-made or natural, can have significant consequences on both humans and the environment. Disasters generally occur without any prior

* Corresponding author.
E-mail addresses: ikhalil@uaeu.ac.ae (I.M. Khalil), akhreish@gmail.com (A. Khreishah), f.ahmed@uaeu.ac.ae (F. Ahmed), k.shuaib@uaeu.ac.ae (K. Shuaib).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.06.002

information or sufficient time to react. In most cases, such devastating events lead to the loss of electricity, damage of communication infrastructure, and failure of Internet connectivity. In most disasters there is always chaos on the ground and workers dealing with humanitarian efforts heavily rely on the available communication options. In case of a disaster such as flood, terrorist attack, or earthquake, the loss of communications increases the hurdle in carrying out humanitarian and relief operations. Therefore, emergency rescue operations must take place without relying on any existing communication infrastructure while rapidly deploying alternative needed communication networks. In this case, WASNs are viable option because even if the infrastructure is damaged there is still likelihood of establishing communication channels which help in executing the humanitarian and rescue operations. Additionally, the pre-deployment of battery-operated WASNs in areas prone to natural disasters or attractive to malicious adversaries prove to be very useful in providing the necessary communication infrastructure needed during the rescue operations. For example, WASN disaster relief applications can provide an effective system to detect living human beings to help successfully manage a disaster relief operation, potentially saving hundreds of lives. Therefore, we have witnessed an increasing number of WASN applications especially developed for humanitarian relief after disasters [21,22].

Recently, the increasing reliance on WASNs has made them *attractive* to malicious attackers, especially terrorist groups, in a bid to hamper rescue operations to amplify the damage and increase the number of casualties. Additionally, the open nature, the fast deployment practices, and the possible hostile environments where the rescue operations may take place, make WASNs *vulnerable* to a wide range of security attacks. Examples of such attacks include data disruption attacks such as complete or selective packet dropping, called blackhole and grayhole respectively, and misrouting in which the attacker relays packets to the wrong next-hop. These attacks could result in a significant loss of data or degradation of network functionality, through the disruption of network connectivity and the prevention of route establishment. A severe instantiation of data disruption attacks is the *Identity Delegation* attack, in which the adversary can drop packets, evade detection, and frame innocent nodes for dropping the traffic.

To decrease human fatalities during disaster recovery efforts, it is extremely important to ensure that WASNs deployed to help rescue teams in such circumstances be reliable and secure. Any natural or malicious disruption of the data flow may critically hinder the rescue process and could increase the number of causalities. In this work, we first discuss the use of WASNs in disaster recovery and management effort and argue that WASNs are a viable option in absence of other communication mechanisms. Then, we discuss the issues of intentional damages to the WASNs from malicious users or terrorists in a bid to further increase the damages. For the purpose of its criticality we analyze one of the possible threats called "*Identity Delegation*" attack and provide a mechanism to handle and prevent this attack.

Being able to monitor and effectively deal with a large number of casualties is vital to the success of a disaster recovery and response scenario. The first responders to a disaster situation need the proper means to fast locate, classify and triage the insured and to better manage the available resources [24]. In the absence of infrastructure based communication technologies, deploying WASN provide an important resource for the first responders to achieve their goals. The use of wireless sensors forming an ad hoc network in disaster effort can span many applications. The most obvious application is maintaining communication among the rescue team personnel on the ground to coordinate their efforts. Another, application is when wireless sensors are used to monitor the insured and report medical data to the medical staff. Doing that contributes to the effective, proper and on time treatment of the insured resulting in fewer casualties. An important aspect of this is to identify and treat the most critically injured first. In addition, collected data can be stored for further treatment when reaching a hospital.

Depending on the nature of the disaster, WASN could be used for a single application or for several ones simultaneously. For example, aside from the medical application, WSAN can also be utilized in monitoring changes in a physical infrastructure to predict further destruction and prevent additional casualties. In flooding situations, WSAN can be used to monitor and report water levels and locate strangled people by tracking signals coming from their cell phones or wearable sensors. In situations where sending humans closer to the disaster event is not an option for safety or other reasons, WASN can be used to evaluate the developing situation on the ground and provide needed information for better assessment and decision making. For example, the authors in [25] used WASN under extreme weather conditions for volcano hazard monitoring. The results obtained from this experimental work showed how resilient such affordable wireless sensor networks could be. Another example could be the use of WASN in nuclear disasters to measure safety radiation levels not necessarily in the heart of the disaster area but on the skirts to evaluate evacuation options and procedures. Fig. 1 summarizes how WASN can be used in various disaster recovery efforts.

In order to mitigate data disruption attacks against WASNs, researchers have used the concept of behavior-based detection, which relies on observing the behavior of neighboring nodes and flagging anomalous patterns. The notion of behavior is related to communication activities such as forwarding packets (e.g., [4]) or non-communication activities such as reporting sensed data (e.g., [14]). A widely used instantiation of behavior-based detection techniques is a state-of-the-art mechanism called Basic Local Monitoring (BLM) (e.g., [1,2,4–6,11,12]). In BLM, a node leverages the open broadcast nature of wireless communication to overhear traffic going in and out of its neighbors. Each node performs different types of checks on the locally observed traffic to identify suspicious behavior. For example, a node may check whether its neighbor relays a data packet to the correct next-hop node, within acceptable delay bounds. For systems where arriving at a common view is important, the detecting node initiates a distributed protocol to disseminate the alarm. Many protocols have