ISSN:0975-9646

Improved secured routing in *Adhoc*Sensor Network for Emergency Medical Care

Anjani Yalamanchili ,DeepthiKethineni , Dukkipati Padma Bhushan

VKR,VNB& AGK College of Engineering,Gudivada, Andhra Pradesh, India

Abstract-To give timely health information, reminders, and support – potentially extending the reach of health care by making it available Wireless ad-hoc networks will enable emergency services to continuously overview and act upon the actual status of the situation by retrieving and exchanging detailed up-to-date information between the rescue workers. Deployment of high-bandwidth, robust, self-organising ad-hoc networks will enable quicker response to typical what/where/when questions, than the more vulnerable communication networks currently in use.This paper addresses network layer protocols for sensor networklike epidemic can be applied but overhead is an issues and also discuss data gathering and aggregation of the Easy Wireless project that enable high bandwidth robust ad-hoc networking.

Keywords— **Epidemic , MCE, EMT ,Data-centric**

I.INTRODUCTION

Our focus is on routing security in wireless sensor networks. Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks. IN emergency situations,security as a goal, we feel it is important to analyse theirsecurity properties. When the VICTIM has the liabilities ofinsecure wireless communication, limited node capabilities,and possible insider threats, and the adversaries can use powerfulnetwork with high energy and long range communicationto attack the network, designing a secure routing protocol isnon-trivial.However, this is non-trivial to fix: itis unlikely a sensor network routing protocol can be madesecure by incorporating security mechanisms after designhas completed. Our assertion is that sensor network routingprotocols must be designed with security in mind, and thisis the only effective solution for secure routing in sensornetworks.SothatIN emergency situations, it is of vital importance forrescue personnel to obtain an accurate and consistentpicture of the situation, and to regain control and coordination on the shortest possible notice. This preventsfurther escalation, minimises the number of casualtiesand restricts the damage. The communication systemsthat are available now for rescue services lack crucialfunctionalities. They suffer from high vulnerability dueto the fact that they rely on a fixed infrastructure andlack of self-organization capabilities, do not supportmultimedia applicationsasking for high qualitycommunications and/or high bandwidth. This technology has the potential to have enormousimpact on many aspects of emergency medical care.Sensor devices can be used to capture continuous, real-timevital signs from a large number of patients, relaying the datato handheld computers carried by emergency medical technicians (EMTs), physicians, and nurses. Wearable sensor nodescans&storepatient data such as identification, history, and treatments, supplementing the use of back-end storage systemsand paper charts. In a mass casualty event (MCE), sensornetworks can greatly improve the abilityof first respondersto triage and treat multiple patients equipped with wearablewireless monitors. Such an approach has clear benefits forpatient care but raises challenges in terms of reliability and complexity. We make five main contributions. We show, for the first time, how attacks against ad-hoc wireless networks and peer- to -peer networks [1], [2] can be adapted into powerful attacks against sensor networks. We present the first detailed security analysis of all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks. We describe practical attacks against all of them that would defeat any reasonable security goals. We discuss countermeasures and design considerations for secure routing protocols in sensor networks

II.BACKGROUND

We use the term *sensor network* to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. Sensor networks may consist of hundreds or thousands of low-power, low-cost nodes, possibly mobile but more likely at fixed locations, deployed en masseto monitor and affect the environment. For the remainder of this paper we assume that all nodes' locations are fixed for the duration of their lifetime. For concreteness, we target the Berkeley Tinos sensor platform in our work. Because this environment is so radicallydifferent from any we had previously encountered, we feel it is instructive to give some background on the capabilities of the Berkeley Tiny OS platform.

A representative example is the Mica *mote*2, a small (several cubic inch) sensor/actuator unit with a CPU, power source, radio, and several optional sensing elements. The processor is a 4 MHz 8-bit Atmel ATMEGA103 CPU with 128 KB of instruction memory, 4 KB of RAM for data, and 512 KB of flash memory. The CPU consumes 5.5 am (at 3 volts) when active, and two orders of magnitude less power when sleeping. The radio is a 916 MHz low-power radio from RFM, delivering up to 40 Kbps bandwidth on a single shared channeland with a range of up to a few dozen meters or so. The RFM radio consumes 4.8 am (at 3 volts) in receive mode, up to 12 am in transmit mode, and 5A in sleep mode. An optional sensor board allows mounting of a temperature sensor, magnetometer, accelerometer, microphone, sounder, and other sensing elements. The whole device is powered by two a batteries, which provide approximately 2850 am hours at 3 volts. Sensor networks often have one or more points of centralized control called *base stations*. A base station is typically a gateway to another network, a powerful data processing orstorage centre, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. In some previous work on sensor network routing protocols, base stations have also beenreferred to as *sinks*.

Base stations are typically many orders of magnitude more powerful than sensor nodes. They might have workstation or laptop class processors, memory, and storage, AC power, and high bandwidth links for communication amongst themselves. However, sensors are constrained to use lower-power, lower bandwidth, shorter-range radios, and so it is envisioned that the sensor nodes would form a multi-hop wireless network to allow sensors to communicate to the nearest base station.

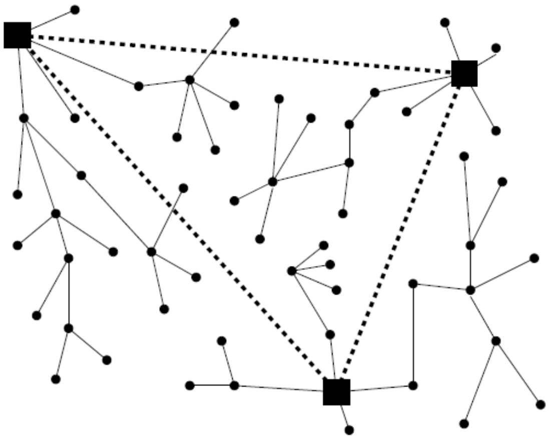


Fig1 A picture illustrating a representative architecture for sensor networks.

A base station might request a steady stream of data, such as a sensor reading every second, from nodes able to satisfya query. We refer to such a stream as a *data flow* and to the nodes sending the data as *sources* .In order to reduce the total number of messages sent and thus save energy, sensor readings from multiple nodes may be processed at one of many possible *aggregation points*. An aggregation point collects sensor readings from surrounding nodes and forwards a single message representing an aggregate of the values. Aggregation points are typically regular sensor nodes, and their selection is not necessarily static. Aggregation points could be chosen dynamically for each query or event, for example. It is also possible that every node in the network functions as an aggregation point, delaying transmission of an outgoing message until a sufficient number of incoming messages have been received and aggregated.

Power management in sensor networks is critical. At full power, the Berkeley Mica mote can run for only two weeks or so before exhausting its batteries. Consequently, if we want sensor networks to last for years, it is crucial that they run at around a 1% duty cycle (or less). Similarly, since the power consumption of the radio is three orders of magnitude higher when transmitting or listening than when in sleep mode, it is crucial to keep the radio in sleep mode the overwhelming majority of the time. It is clear that we must discard many preconceptions about network security: sensor networks differ from other distributed systems in important ways. The resource-starved nature of sensor networks poses great challenges for security. These devices have very little computational power: public-key cryptography is so expensive as to be unusable, and even fast symmetric-key ciphers must be used sparingly. With only 4KB of RAM, memory is a resource that must be husbanded carefully, so our security protocols cannot maintain much state. Also, communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800–1000 instructions [3], and as a consequence, any message expansion caused by security mechanisms comes at significant cost. Power is the scarcest resource of all: each milliamp consumed is one milliamp closer to death, and as a result, nearly every aspect of sensor networks must be designed with power in mind. Lest the reader think that these barriers may disappear in the future, we point out that it seems unlikely that Moore's law will help in the foreseeable future. Because one of the most important factors determining the value of a sensor network

comes from how many sensors can be deployed, it seems likely there will be strong pressure to develop ever-cheaper sensor nodes. In other words, we expect that users will want to ride the Moore's law curve down towards ever-cheaper systems at a fixed performance point, rather than holding price constant and improving performance over time. This leaves us with a very demanding environment. How can security possibly be provided under such tight constraints? Yet security is critical. With sensor networks being envisioned for use in critical applications such as building monitoring, burglar alarms, and emergency response, with the attendant lack of physical security for hundreds of exposed devices, and with the use of wireless links for communications, these networks are at risk.

III.NETWORKS PROTOCOLS

we apply ad hoc networks protocols like epidemic can be applied but overhead is an issue" Aims are usually different: not communication but data reporting to single or multiple source" Specific protocols have been devised"Specific nodes are interested in specific events"Sink interested in all results"Sink interested in a sensor reading change"

PROTOCOLS FOR REPEATED INTERACTIONS

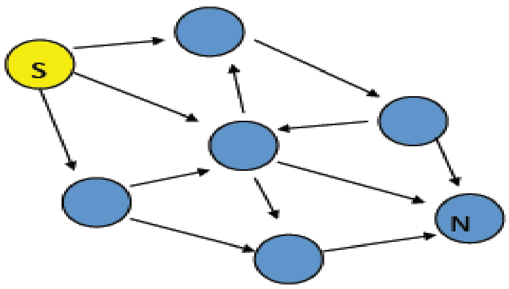
Subscribe once, events happen multiple times"Exploring the network topology might actually pay off" But: unknown which node can provide data, multiple nodes might ask for data"! How to map this onto a "routing" problem?"**Idea:** Put enough information into the network so that publicationsand subscriptions can be mapped onto each other" But try to avoid using unique identifiers: might not be available,might require too big a state size in intermediate nodes"! ***Directed diffusion*** as one option for implementation" Rely only on ***local interactions*** for implementation".

Data-centric approach

- Nodes send "interests" for data which are diffused in the network"
- Sensors produce data which is routed according to interests"
- Intermediate nodes can filter/aggregate data"

Interest propagation

Each sink sends expression of interests to neighbours. Each node will store interests and disseminate those further to their neighbors.(Cache of interest is checked not to repeat disseminations).
Interests need refreshing from the sink [they time out].Interests have a "rate of events" which is defined as **"gradient"!**



Data delivery

Sensor data sources emit events which are sent to neighbors according to interest [i.e. if there is a gradient].Each intermediate node sends back data at a rate which depends on the gradient" I.e. if gradient is 1 event per second and 2 events per second are received send either the first or a combination of the two[aggregation].Events are stored to avoid cycles [check if same event received before].Data can reach a node through different paths. Gradient enforcement needed.

GRADIENTS REINFORCEMENT

When gradients are established the rate is defined provisionally[usually low].Sinks will reinforcegood paths which will be followed with higherrate.
A path expires after a timeout so if not reinforced it will cease to exist" This allows adaptation to changes and failures.

Directed diffusion – Two-phase pull

Phase 1: nodes distribute ***interests*** in certain kinds of named data.Specified as attribute-value pairs. Interests are flooded in the network. Apparently obvious solution: remember from where interests came, set up a “tree”.Problem: Node X cannot distinguish, in absence of unique identifiers, between the twosituations on the right – set up only one or three trees.

Direction diffusion – Gradients in two-phase pull

Option 1: Node X forwarding received data to all “parents” in a “tree” .Not attractive, many needless packet repetitions over multiple routes.

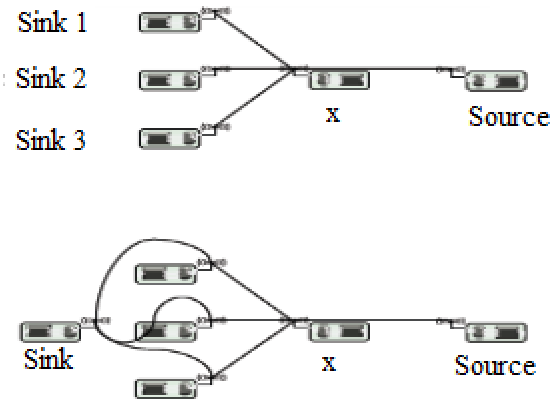


Fig 2:

Option 2: node X only forwards to one parent
Not acceptable, data sinks might miss events
Option 3: Only provisionally send data to all parents, but ask data sinks to help in selecting which paths are redundant, which are needed Information from where an interest came is called ***gradient***" Forward all published data along all existing gradients"

Directed diffusion – extensions

- Problem: Interests are flooded through the network"
- Geographic scoping & directed diffusion .Interest in data from specific areas should be sent to sources in specific geo locations only"
- Push diffusion – few senders, many receiver Same interface/naming concept, but different routing protocol. Here: do not flood interests, but flood the (relatively few) data .Interested nodes will start reinforcing the gradients

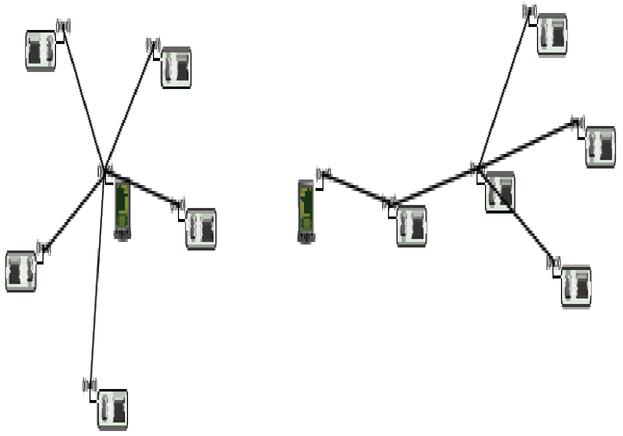
Issues

- Purely theoretical work
- A part from the flooding of the interests
- No consideration of real world issues such as link stability or link load and load dependence
- Mac Layer issues (assume nodes are awake or does not discuss it)
- More recent approaches have considered link capabilities as part of the routing decision making

Data aggregation

- Less packets transmitted -> less energy used"
- To still transmit data, packets need to combine their data into fewer packets ***aggregation***is needed

•Depending on network, aggregation can be useful or pointless
• Directed diffusion gradient might require some data aggregation.



Metrics for data aggregation

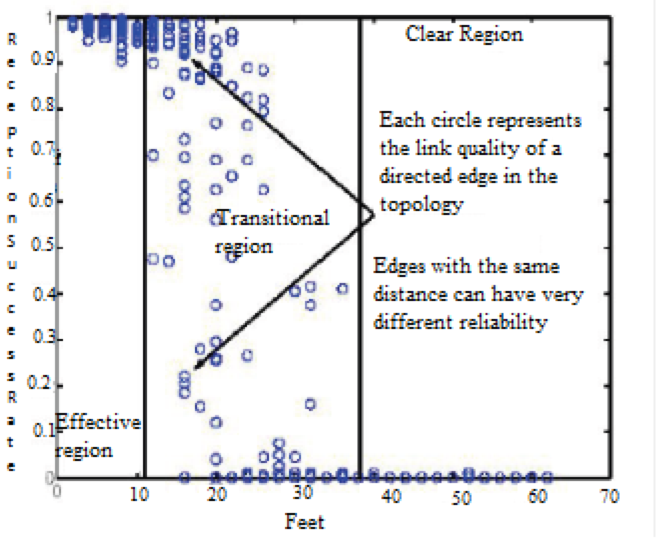
• ***Accuracy***: Difference between value(s) the sink obtains from aggregated packets and from the actual value (obtained in case no aggregation/no faults occur)
• ***Completeness***: Percentage of all readings included in computing the final aggregate at the sink
• ***Latency***
• ***Message overhead!***

Link quality based routing

• Directed diffusion uses some sort of implicit ways to indicate which are the good links. Through the gradient.
• Ad hoc routing protocols for mobile networks route messages based on shorter path in terms of number of hops.
• The essence of the next protocol we present: "number of hops might not be the best performance indication in wireless sensor network.

Routing based on Link Estimation.

• Routing algorithms should take into account underlying network factors and under realistic loads.
• Link connectivity in reality is not spherical as often assumed.



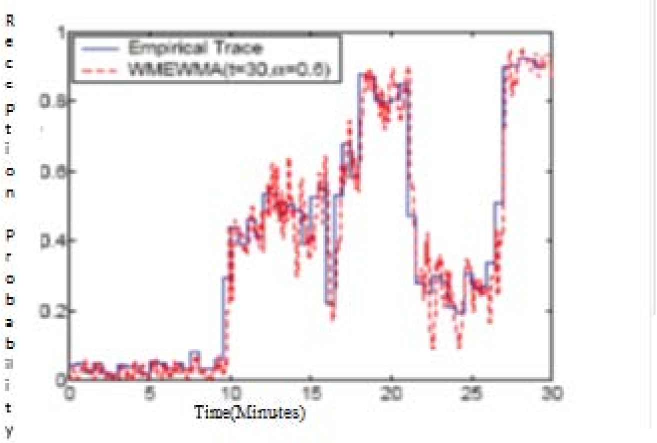
Link Estimation

A good estimator in this setting must be stable. Be simple to compute and have a low memory foot print. React quickly to large changes in quality. Neighbour broadcast can be used to passively estimate.

WMEWMA

Snooping Tracks the sequence numbers of the packets from each source to infer losses. Window mean with EWMA "MA(t) = (#packets received in t) / max(#packets expected in t, packets received in t)","EWMA(TX)=a (MA(TX)) + (a-1)EWMA(t(x-1))".TX : last time interval; a: weight"

WMEWA (t =30, a =0.6)"



Neighbourhood Management

Neighbourhood table Record information about nodes from which it receives packets(also through snooping).If network is dense, how does a node determine which nodes it should keep in the table.To Keep a sufficient number of good neighbours in the table. Similar to cache management for packet classes.

Link Estimation based Routing

- Focus on "many to one" routing model Information flows one way. Estimates of inbound links are maintained, however outbound linksneed to be used." Propagation back to neighbours". Each node selects a parent [using the link estimation table].Changes when link deteriorates (periodically).

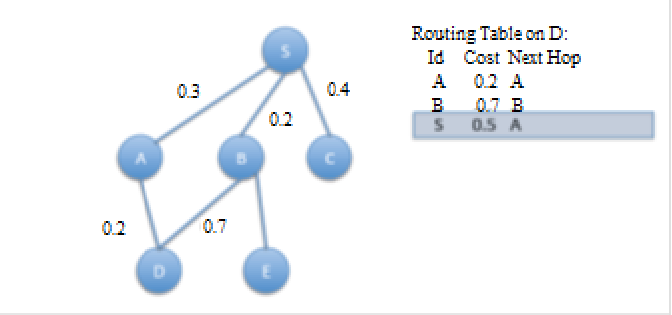
Distance vector routing

cost metrics

Routing works as a standard distance vector routing. The DVR cost metric is usually the hop count. In lossy networks hop count might underestimate costs. Retransmissions on bad links: shortest path with bad links mightbe worse than longer path with good links. Solution: consider the cost of retransmission on the whole path.

MIN-T"

MT (Minimum Transmission) metric. Expected number of transmissions along the path for each link, MT cost is estimated by (1/(Forward link quality) * 1/(Backward link quality))backward links are important for asks. Use DVR with the usual hop counts and MT weights on links.



Routing Table on D:

Id	Cost	Next Hop
A	0.2	A
B	0.7	B
S	0.5	A

I. Conclusions

The main advantage of this new model being proposed is that it provides secured routing in AdHoc Sensor Networks for Emergency medical care. In order to ensure application of this model in amore generalized manner, we need to replicate this study on other larger project s in addition to assessing the validity of the model for predicting the confidentiality, fault proneness and maintain ability. Deployment of high –band width , robust, self –organizing adhoc network s will enable quicker responses in use .secure routing is vital to the acceptance and use of sensor network s for many applications, but we have demonstrated that currently proposed routing protocols for these networks are in secure.We leave it is as an open problem to design a sensor network routing protocols that satisfies our proposed security goals

Acknowledgment

In this chapter, we considered the two security services of authentication relating to authentication and confidentiality, specific to ad hoc networks, have been identified and the characteristics of these services have been outlined. The proposed security solutions for the two services of authenticationand confidentiality have been categorized into three categories, depending upon the underlying security techniques. Proposed solutions within each category are discussed in detail. Finally, IEEE 802.11i, standard for wireless security is detailed, its vulnerabilities are highlighted and the solutions proposed for the vulnerabilities are discussed. The chapter ends witha note on the open issues relating the two security issues of authentication and confidentiality in wireless ad hoc networks.

References

[1] GMP Wireless Medicine, Inc. `http://www.wirelessecg.com/`.
[2] HealthFrontier, Inc. `http://www.healthfrontier.com/Products/`.
[3] Nonin Medical, Inc. `http://www.nonin.com/`.
[4] Numed Holdings Ltd. `http://www.numed.co.uk/`.
[5] Radianse, Inc. `http://www.radianse.com/`.
[6] Telos corporation.`http://www.telos.com/`.
[7] 10Blade, Inc. iRevive. `http://www.10blade.com/irevive.html`.
[8] Inc. Crossbow Technology. Motes, smart dust sensors, wireless sensor networks. `http://www.xbow.com/Products/productsdetails.aspx?sid=3`.

[9] Jason Hill, Robert Szewczyk, Alec Woo, Seth Hollar, David E. Culler, and Kristofer S. J. Pister. System architecture directions for networked sensors. In *Architectural Support for Programming Languages and Operating Systems*, pages 93–104, 2000.
[10] Institute of Electrical and Electronics Engineers, Inc. IEEE 802.15.4.draft standard. `http://grouper.ieee.org/groups/802/15/pub/TG4.html`.
[11] David Malan. Crypto for tiny objects. Technical Report TR-04-04, Harvard University, January 2004.
[12] Microsoft Corporation. Microsoft .NET Compact Framework.`http://msdn.microsoft.com/mobility/prodtechinfo/devtools/netcf/`.
[13] The MobiHealth Project. Innovative gprs/umts mobile services for applications in healthcare. `http://www.mobihealth.org/`.
[14] Matt Welsh and Geoff Mainland. Programming sensor networks using abstract regions. In *the First USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI '04)*, March 2004.
[15] Alec Woo, Terence Tong, and David Culler. Taming the underlying challenges of reliable multihop routing in sensor networks. In *the First ACM Conference on Embedded Networked Sensor Systems (SenSys 2003)*, November 2003.