Enabling Large Scale Ad hoc Animal Welfare Monitoring

Bartosz Wietrzyk, Milena Radenkovic
School of Computer Science
University of Nottingham
Nottingham, NG8 1BB, UK
e-mail: bartosz@wietrzyk.name, mvr@cs.nott.ac.uk

Abstract— **Automated animal monitoring with energy efficient wireless devices mounted on the animals can improve efficiency of farming industry and increase its profitability by decreasing reliance on human labor. We discuss the practical deployment of delay tolerant store and forward cattle monitoring architecture that provides data retention, detecting custom events, notification issuing, remote and in-situ queries answering. The core of this architecture, a novel energy efficient, disruption tolerant, Mobile Ad Hoc Network (MANET) routing protocol (EERD), provides offloading data for long term storage by sending data to farm servers via sinks that are a part of a MANET and handles in-situ queries issued by users collocated with the animals. The energy efficiency is achieved by dynamic adaptation to the current behavior of the animals carrying the monitoring devices. We discuss the practical feasibility of this architecture by analyzing data from the extensive field experiments we performed. We address the challenges posed by the practical deployment. In particular we propose an energy efficient mechanism for dealing with disconnections and identify potential security threats that include unauthorized fabricating, changing and accessing collected measurements, as well as MANET routing attacks. Finally we propose feasible precautions against these threats and discuss their impact on our energy efficient routing protocol (EERD).**

Keywords- Animal Monitoring, DTN, MANET, Wireless Routing, Security

I. INTRODUCTION

There is a proliferation of interest in using wireless ad hoc technologies to monitor health and behavior parameters of wild, as well as domestic animals [1-7] and the environment as a whole [8]. This paper focuses on cattle monitoring because timely detection of cattle health problems can prevent spread of diseases such as mastitis and other infection diseases, metabolic diseases and lameness, which can lead to decreased productivity and death of valuable stock [2], as well as endanger health of the humans. The productivity of a farming enterprise can be also extended by timely detection of the oestrus in order to efficiently perform insemination of cows. Currently most of the farms practice manual observation, whereas the most advanced enterprises utilize milk monitoring by stationary sensors, or animal mounted sensors read over a single hop communication having very short [9] to medium range [10] leading to disconnections. These solutions are simple and easy to implement but require expensive infrastructure to provide full coverage or they offer only limited reliability. Current state of the art research for monitoring cattle behavior and metabolism in the Wireless Sensor Networking (WSN) research community are largely pragmatic proofs of concepts [11]. More precisely they utilize single hop [4, 5] or GSM communication [2]. The latter is expensive and not reliable in agricultural areas, where GSM operators have limited incentives to provide complete coverage.

In this paper, we discuss practical feasibility of the deployment of the delay store and forward architecture introduced in [7, 12], that provides data retention, detecting custom events, notification issuing, remote and in-situ queries answering. The core of this architecture, a novel energy efficient, disruption tolerant Mobile Ad Hoc Network (MANET) routing protocol provides offloading data for long term storage by sending data to farm servers via sinks that are a part of a MANET and handles in-situ queries issued by users collocated with the animals. The advantages of this protocol are following: (1) we significantly optimize energy efficiency of control traffic by identification and utilization of animal movement patterns, as well as graceful degradation of data traffic energy efficiency, (2) the protocol can dynamically adapt to the current behavior of the animals carrying the mobile devices, (3) it can work with any type of bovine animals. Reducing and balancing energy utilization of the mobile nodes is essential from the perspective of farming industry because it allows decreasing labor necessary for changing the batteries installed in the animal mounted devices.

In this paper, we demonstrate practical feasibility of this algorithm by extended monitoring of behavior of 5 animals over 1 year. Our results are based on significantly larger data set than normally used for this kind of application domain. The usual data size would sometimes include a somewhat bigger number of nodes but would in turn have much shorter time span of the data capture (weeks rather than months of years). Finally we address the challenges of the practical deployment of the proposed algorithm by proposing mechanism for dealing with disconnections and discussing

the security issues. We argue that security issues are at the core of allowing deployment of the cattle monitoring in the commercial environment. Competitors are likely to disrupt functioning of the target farming enterprise or put it into a less favorable position. Buyers of the animal products (e.g., supermarkets) may want to lower the price of the products they buy or gather intelligence about the sellers to better evaluate their offer. The impact of the utilized security precautions on the energy efficiency of the animal mounted devices should be minimized.

This paper builds upon our earlier publication [7] by providing extended experimental data and analysis of this data, introducing disconnection handling to our energy efficient routing algorithm EERD, discussing security threats against the proposed cattle monitoring system and possible precautions against these threats. The paper is organized as follows. Section 2 discusses and categorizes related work. Section 3 presents the proposed architecture. Section 4 reports on the setup and results of our field experiments we performed to collect realistic data sets and requirements necessary to evaluate the proposed architecture and the MANET routing protocol. The cattle movement data from these experiments was uploaded [13] to the Community Resource for Archiving Wireless Data At Dartmouth (CRAWDAD). Section 5 presents our practical protocol that provides data off-load and in-situ queries extending the discussion about combating disconnections. Section 6 identifies potential security threats, proposes feasible precautions against them and discusses impact of these precautions on the proposed protocol. Finally, Section 7 identifies future challenges.

II. Related Work

This section discusses existing Wireless Sensor Networks (WSNs) for animal monitoring. The WSNs [14] consist of hundreds to thousands of inexpensive wireless nodes, each with some computational power and sensing capability, operating in an unattended mode. The hardware technology for these networks are low cost processors, miniature sensing and radio modules. Sensor data includes continuous sensor readings of physical phenomena, audio and video streams.

a) Stationary Wireless Sensor Networks. The initial WSNs were purely stationary. The sensor data was archived in a powerful server geographically collocated with the sensors (usually referred to as a base station) that was usually fully replicated on the pre-determined powerful servers in the labs. Users could query the databases to get information about sensor data. An example stationary WSN was the WSN deployed on the Great Duck Island [15] to monitor the ecology of Leach's Storm Petrel. It used single-hop communication and had a multi-layer architecture. The fist layer consisted of multiple sensor networks that were deployed in dense patches that were widely separated and measured various physical phenomena and had cameras and microphones. Each sensor patch had sensor motes that were capable of various forms of filtering, sharing and combining sensor measurements. Sensor motes transmitted sensor data to the second layer that is referred to as a gateway. A gateway was then responsible for transmitting the packets to the third level referred to as the base station and some further data processing. The base station in the third level provided full database services and connectivity to the database replicas across the Internet. Fourth layer usually refers to services that provide multi-user access to sensor data including services for supporting analysis, visualization and web content. Once deployed, most base stations are intended to remain stationary and in a densely packed configuration. WSN deployed on the Great Duck Island comprised 43 sensor nodes and its maintenance was characterized by low labor intensity. Its stationary character allowed simplification of the routing and avoiding problems with mobility and disconnections. The simple routing and lack of disconnections helped in avoiding problems with energy saving. Lack of disconnections and problems with energy saving allowed short delays. This approach because of its stationary character does not apply to our scenario.

b) Animal Mounted. In a typical animal mounted WSN mobile nodes send measurements to a centralized server over a GSM or satellite network. Alternatively the measurements are collected by a mobile base station carried by a human or mounted on a vehicle and then manually processed [1]. The oldest form of animal mounted wireless sensors are radio tags, which send VHF beacons [16]. Their measurements are retrieved by a base station which can be fixed, carried by a human or mounted on a vehicle. This approach is not optimal for our scenario because using fixed base stations is expensive in the case of covering larger areas. Using base stations carried by humans or mounted on vehicles is very labor intensive. In both cases potentially data from only a subset of tagged animals can be retrieved. The more recent variant of this method [16] is using satellite telephony instead of VHF beacons. This is much less labor intensive and more reliable but also very expensive and energy inefficient. One of the first examples of animal mounted WSNs was ZebraNet [1] that consisted of animal mounted collars collecting and exchanging GPS locations, which were retrieved by a mobile base station. The collars were opportunistically exchanging all stored measurements with all encountered nodes. This addressed disconnection but had low scalability – the maximal envisaged number of the deployed animal mounted nodes was 30 and involved human labor. The authors of [2] mounted various sensors on a single steer to monitor temperature inside its rumen, location, acceleration, as well as external temperature, humidity and pressure. The measurements from the sensors were transmitted to the gateway mounted on the animal, which forwarded them on via GPRS. The presented approach was expensive and not energy efficient because of extensive utilization of GPRS. Low energy efficiency increased the labor intensity of its maintenance. The GSM telephony can have limited coverage in rural areas where the cattle is kept [2]. This approach does not address our requirements because due to heavy utilization of GSM it has high costs and low energy efficiency. Butler et al. [3]

proposed using animal mounted devices to force bovine animals to move or stay within virtual fences but did not address the energy efficiency of the wireless communication. Researchers at CSIRO [4, 5] fitted 13 cows with collars containing accelerometers, GPS receivers and wireless networking interfaces in order to examine reliability of the communication and usability of the data collected by GPS receivers and accelerometers. The authors did not give the details about the utilized routing protocol and did not consider the energy efficiency. The later work of these researchers [6] concerns using animal mounted devices to prevent bulls from fighting with each other. The animal mounted collars have GPS receivers, wireless network interfaces and are capable to apply electric shocks to the animals wearing them. The utilized wireless communication is a simple single-hop one without considering energy efficiency. Small et al. [17-19] proposed using whale mounted sensors to collect data about whales and their habitat. They utilized a combination of the Infostation [20, 21] paradigm and a DTN approach similar to Gossiping [22]. This work is similar the ZebraNet [1] but limits the probability of forwarding data to other nodes. In our scenario animal mounted devices form a much denser topology than in the case of whale monitoring. Therefore, gossiping would increase the network overhead and thus affect energy efficiency.

c) DTN networks for rural areas. There is intensive ongoing research in DTN networks for rural developing areas [23-26]. However, this research typically concerns providing connectivity between villagers or between villagers and local authorities rather than monitoring farm animals and does not consider energy efficiency.

III. Architecture of the Cattle Monitoring System

This section describes the architecture of the target cattle monitoring system, more fully described in [12, 27]. The scope of the monitoring system is a farming enterprise, which comprises several pastures and barns where animals are kept. The cattle can be kept all the year continuously in the pastures or all the year in the barns but the most common practice is to keep them in the pastures during the warmer half of the year and indoors during the other [28]. The proposed system can be used to monitor animals regardless if they are kept continuously in the pastures or in the barn and regardless if they currently yield milk or not.

An animal mounted device has the form of a collar with a built-in accelerometer measuring the intensity of feed intake. Walking intensity is measured by a pedometer mounted on the animal's leg. Measurements from the pedometer are acquired by the collar over wireless communication. Measurements from the pedometer and accelerometer are stored and processed by the collar. Both the collar and the leg mounted pedometer are battery powered. Data processing performed by animal mounted devices aims to detect oestrus, pregnancy, animal diseases etc. They have wireless network interfaces and regularly transmit raw and processed data to the farm servers over the sinks. Sinks are members of the MANET which forward the data collected and processed by animal mounted devices to farm servers. Animals wear the same devices regardless if they are kept in pastures or barns.

The typical amount of data for each update sent from animal mounted devices to sinks is 32B. As shown in Figure 1, sinks can be connected to farm servers over a wired network connection or GSM telephony. In the latter case, the sink can be stationary or animal mounted. The farm servers store the real time and historic data, detect the user defined events and issue notifications about these events.

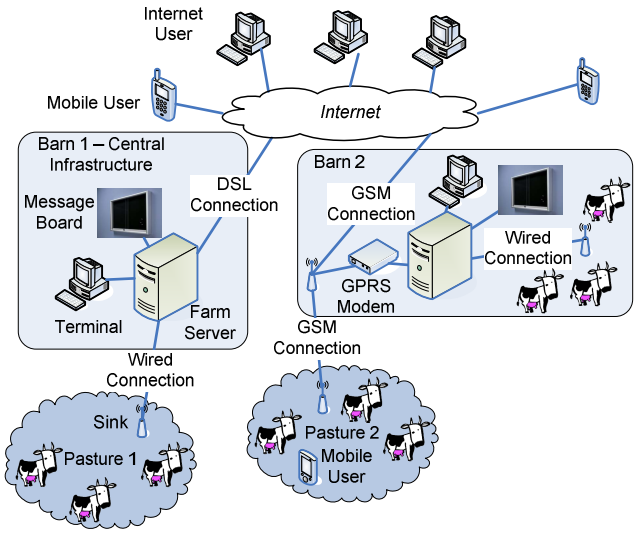

Figure 1. Example deployment

The users can query the data stored on the servers, including raw and processed data, either locally at the farm or remotely over the Internet. Users located in a pasture, stall or in its close proximity may want to query data about the animals located there. This can be achieved by querying the data from a PDA or a smart phone connecting directly to the animal mounted devices, or via the sinks over the wireless communication.

IV. Field Experiments

In this section, we describe field experiments we performed at the University of Nottingham's Dairy Centre in collaboration with School of Biosciences. The purpose of these field experiments was collection of realistic data sets necessary to evaluate the practical feasibility of the delay tolerant architecture and the energy efficient MANET routing protocol for the cattle monitoring system. The cattle movement data from these experiments was uploaded [13] to the Community Resource for Archiving Wireless Data At Dartmouth (CRAWDAD). CROWDAD is an international repository of real wireless data for wireless network research community.

A. Experiment Setup

Field experiments comprised cattle movement and behavior monitoring in order to gather the realistic

environmental constrains. We received one year long walking intensity data from 5 pedometers mounted on the cows located in the division of a modern dairy housing 100 animals, shown in Figure 2. Cows could move freely in the area with feeder, water tank, resting bays and milking robots available 24 hours a day. Their measurements were automatically collected by milking robots whenever a cow was milked.

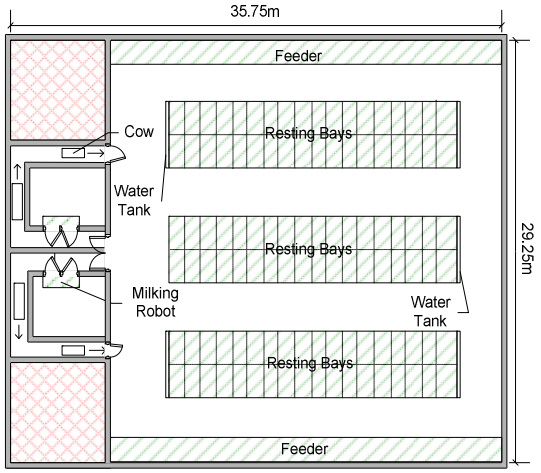

Figure 2. Layout of the dairy division

We also monitored behavior of the animals using animal mounted GPS receivers and cameras. In particular we mounted on the monitored cows five collars, each comprising a neck strap and an aluminum instrument enclosure containing a Bluetooth GPS and a Bluetooth enabled mobile phone. Mobile phones were logging data from the GPS receivers including positions and timestamps. Monitoring started at 11:10. The collars were removed at 18:10. GPS receivers worked until 18:24 (manually turned off), 12:23 (probably jammed), 18:51 (manually turned off), 15:09 (exhausted battery), 15:33 (exhausted battery). Later we submitted [13] the collected GPS and pedometer data to the Community Resource for Archiving Wireless Data At Dartmouth (CRAWDAD). Concurrently we were filming the part of the dairy where the monitored cows were kept. We placed the camera on two ramps above this area. These locations offered the most complete view. We received the plan of the dairy and then captured the coordinates of the characteristic locations on the plan using a handheld GPS receiver. GPS receivers and filming were utilized only for the purpose of our field experiments. Their utilization is not intended for the target monitoring system.

B. Results

Our field experiments show that cows typically react well to the animal mounted collars weighting 1075g. This is very promising for the practical feasibility of the target cattle monitoring system. Figure 3 shows the average daily walking intensity of five cows, calculated from the one year long pedometer data as arithmetic weighted mean of walking intensities per each cow and each day. We can see that the animals' mobility can differ significantly among different animals and for each animal among different days. However, from this picture we cannot judge how the walking intensity is reflected in the spatial mobility. Figure 4 shows probability distribution of speeds for a subset of cows wearing GPS receivers. They were calculated by dividing the time a cow used the given speed range by the length of time the GPS receiver was enabled. We can see that not only walking intensity but also the preferred spatial movement speed can significantly differ among animals. These considerable differences in the animals' walking speed are utilized in our routing protocol (see Section 5.B.2a). Figure 4 also shows that the animals rarely move faster than 0.8 m/s, which is important for the wireless communication.

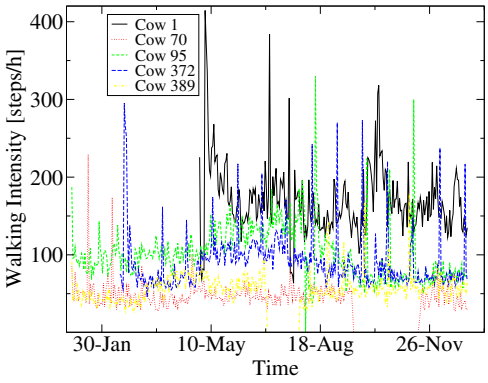

Figure 3. Walking intensity (pedometers)

Figure 5 shows average walking intensity over the day for five different animals, each average walking intensity was calculated as a weighted arithmetic mean for each animal and for each hour of the day (i.e., one hour time frame) throughout all the days for which we had pedometer data (one year). Figure 6 shows the probabilities of milking happening at a given hour, calculated as a ratio of milkings number at given hour of the day to the number of all recorded milkings. We can see that cows are active all the day and night including walking and milking but they show similar 24 hours patterns. In particular, walking and milking activities tend to be less intensive between 0 and 6 a.m. These periods can be utilized for scheduled data exchanges. Our algorithm uses 24 hours period to calculate average speed of animals (see Section 5.B.2a).

The quantitative experiments were performed in the dairy but this is only an example deployment scenario of the target monitoring system. The target monitoring system is also intended to monitor beef cattle animals kept continuously on the pastures even all the year. Such cattle may never be taken to the farm buildings.

V. ENERGY EFFICIENT ROUTE DISCOVERY

This section describes realistic, energy efficient MANET routing protocol, Energy Efficient Route Discovery (EERD), for the cattle monitoring system we introduced in [7, 12] and proposes energy efficient mechanism for dealing with disconnections. EERD concerns sending data from animal mounted nodes to sinks and performing in-situ queries. It significantly optimizes energy efficiency of control traffic by

identification and utilization of animal movement patterns, as well as graceful degradation of data traffic energy efficiency. We concentrate on energy utilized for wireless communication because the progress in the energy efficient microcontrollers with high computation power made the energy utilized for data processing negligible [29] in relation to energy spent on wireless communication. Simulation based analysis of delays, latency and package lost were presented in our earlier paper [7]. They show that EERD not only decreases energy utilization but also improves success ratio of packet delivery in relation to DSR [30] and a generic energy efficient routing protocol ESDSR [31]. The improved success ratio is achieved by decreasing packet loss caused by congestion.

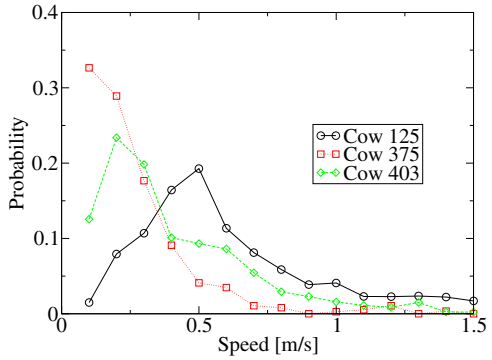

Figure 4. Probability distribution of animal speed (GPS receivers)

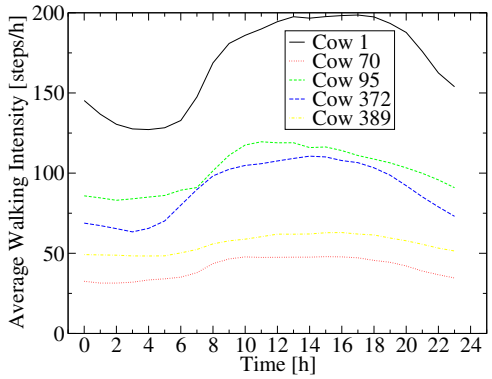

Figure 5. Activity over the day (pedometers)

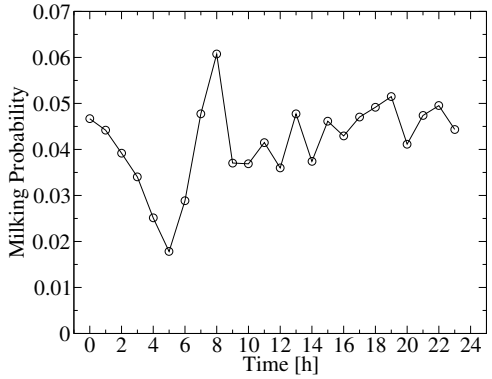

Figure 6. Milking probability (pedometers)

A. *Overview*

Energy Efficient Route Discovery (EERD), for cattle monitoring system minimizes and balances energy consumption in the face of low data traffic and high mobility of nodes. It decreases energy spent on route discovery and in-situ queries by utilization of the tailored PCDI broadcasting. The number of necessary route discoveries is decreased by utilization of heterogeneity of nodes' mobility, selecting routes with longest lifetime and opportunistic route discovery. It is based on the established MANET routing protocol, DSR [30].

EERD balances and saves energy on routing data by monitoring average speed of the nodes, remaining battery capacity of the local node, energy attenuation of the received and overheard packets, as well as acquiring routes from overheard and forwarded packets.

B. *Energy Saving and Route Discovery Techniques*

In this subsection, we describe energy saving and route discovery techniques utilized by EERD.

1) Decreasing and Balancing Energy Spent on Route Discovery

As in ESDSR [31] nodes put the utilized transmitter power in the packets so that each node can track power necessary to contact its single-hop neighbors using the following formula:

$$P_{min} = P_{tx} - P_{recv} + P_{threshold} + P_{margin} \quad (1)$$

where P_{min} is the minimal required power for the sender to use, P_{tx} is the current transmit power, P_{recv} is the current received power, $P_{threshold}$ is the threshold power level for the application, and P_{margin} is the margin to safeguard against changes such as channel fluctuation and mobility. All the values are in dBm. Note that only route requests and other broadcasted packets are sent using the maximal power of the transmitters.

Energy spent on route discovery is minimized and balanced by applying Passive Clustering with Delayed Intelligence (PCDI) [32] to route request broadcasts. Note that broadcasted packets are sent using maximal transmitter power so power of the received broadcasts can still be utilized to calculate PCDI waiting time. In PCDI nodes with higher battery capacity are more likely to route broadcasted packets so discovered routes lead through these nodes. This results in more fair energy utilization of data traffic.

2) Decreasing Number of Route Discoveries

In this subsection, we describe techniques for decreasing number of route discoveries in order to limit energy utilization.

a) Utilizing Heterogeneity of Node's Mobility. The field experiments reported in Section 4 show that there are considerable differences between typical movement speeds and typical walking intensities of animals carrying wireless nodes. The proposed protocol decreases chances that faster wireless nodes become members of the route by delaying their rebroadcasting of PCDI broadcasts. In this way, the

lifetime of the discovered routes is extended so repeated sending of data, route failure packets and route discovery broadcasts can be minimized.

Each mobile node stores the 24 hour time series of its momentary speed received from the pedometer – expressed as number of steps per time unit. An average speed is calculated over this time series discarding time when an animal did not move. The 24 hour time period is motivated by limited resources of the nodes and the 24 hour movement pattern cycle of the animals indicated by the pedometer data (see Figure 5). Each transmitted packet has a piggybacked maximal and minimal average speed of a node. These values are updated and stored by the forwarding nodes. Each node resets these stored values after a timeout to account for the changing conditions. This data allows nodes to asses their mobility in relation to other nodes. In EERD the PCDI formula calculating waiting time is extended by taking into account the average speed of the node in relation to average speeds of other nodes:

$$W = \delta \times \frac{receivedPower}{localEnergy} + \varepsilon \times \frac{V_L - V_{MIN}}{V_{MAX} - V_{MIN}} \quad (2)$$

where δ and ε are constants adjusted for the particular hardware, V_L is the average speed of the local node, V_{MIN} and V_{MAX} are minimal and maximal average speeds of the neighborhood nodes. In this way, relatively faster nodes wait longer to rebroadcast PCDI broadcasts so their probability of becoming PCDI clusterheads or gateways and later forwarding data traffic is smaller.

b) Selecting Routes with Longest Lifetime. The number of route discoveries is further minimized by selecting routes with potentially longest lifetime. Because of the high mobility of the nodes the life of a route is typically terminated not by the exhausted battery capacity but by the change of the topology.

Utilizing received, forwarded and overheard packets a node monitors how the energy attenuation changes between the one hop neighbors. In this way, a node can count how many links within the multi-hop route are increasing their energy attenuation (deteriorating). In particular each forwarded route request and acknowledgement packet contains a counter of deteriorating hops.

Finally, a node selects routes which have (1) *the least number of hops*. For routes with the same number of hops, a node chooses these with (2) *the least number of deteriorating links*. If this is equal one with (3) *the minimal total power* (i.e., sum of the transmitter power necessary to send data over each hop) is selected.

c) Opportunistic Route Acquisition. An important way of limiting the number of route discoveries is collecting routes from overheard and forwarded packets such as route replies and data traffic. The gain from overhearing depends on the utilized wireless networking interface, in particular how much the power consumed by transmitting is greater than the power consumed by receiving and what is the difference in power consumption between promiscuous and non-promiscuous mode.

3) Saving Energy on Broadcasts in In-situ Queries

A mobile user collocated with the animals can issue both regular queries and directed queries. The answer to a regular query is a group of animal ids (or their custom nicknames) that fulfill a given logical condition (e.g., all animals which are sick). Directed queries concern data about a particular animal (e.g., predicted date of the next oestrus). The user broadcasts the query using PCDI with the proposed optimizations. All the nodes that know any partial answer to the query send the answer back to the user, together with the timestamp of the data based on which the answer was generated. The answer is sent back along the route traversed by the query. Nodes that forward the queries assemble and filter these answers according to their timestamps in order to reduce redundant traffic. The final assembly is performed by the user's device.

C. Handling Disconnections

We propose extending EERD with the following mechanism for handling disconnections, which within this paper mean splitting of the network topology into separated islands of connectivity. The proposed protocol is intended to adapt to different environments, where the cattle is kept, dairy, pasture, etc. Therefore, it is not possible to present fixed boundaries of disconnection time.

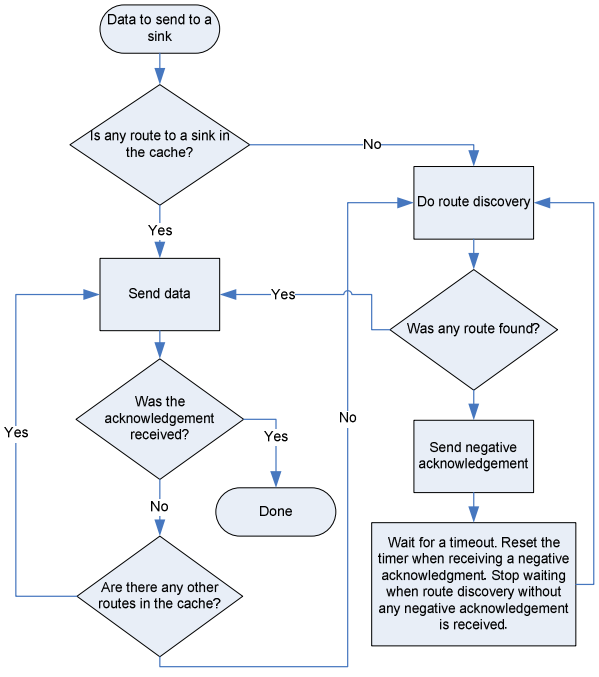

Figure 7. Cooperative detection of route availability

In the case of sending data to sinks the data is sent only when the multi-hop path between an animal mounted node and any of the sinks exists. It is detected using the proposed *cooperative detection of route availability*, shown in Figure

7. More precisely, if the route discovery is unsuccessful it is repeated after a certain timeout with a small random delay. The purpose of the random delay is preventing the broadcast storm caused by multiple nodes initiating route discovery at the same time. In order to save energy on the repeated unsuccessful route discoveries if the route discovery is unsuccessful the node that initiated it broadcasts a negative acknowledgement. In this way, all the nodes within its island of connectivity know that the route to the sink is not available and the route discovery should be repeated no sooner than after the predefined timeout. Otherwise if a node receives a route request packet but no negative acknowledgement, this means that a route to a sink exists so the node can try to discover it. The negative acknowledgements are preferred here over positive ones to save energy in circumstances when no disconnections take place – e.g., animals are located in a barn.

When a sink receives data from an animal mounted node it sends an acknowledgement. If no acknowledgement is received the animal mounted node resends the data over a different path and if it does not know any alternative path it initiates route discovery.

In order to answer the in-situ queries in the face of disconnections the animal mounted nodes should be able to answer the query within the island of connectivity (network partition). To achieve that, nodes cache data sent to sinks which they forward or overhear. This caching is performed according to their available storage space. The proactive caching, i.e., the proactive exchange of the data for the purpose of caching, is not advisable here due to the energy constrains [33]. If the sink is connected to the farm server over an expensive third party connection such as GPRS, it may also cache the data forwarded to farm servers. In this way, the sink can support answering in-situ queries without the need to query the farm server.

Nodes receiving an in-situ query answer it whenever they have at least a partial answer to this query. This answer can come from locally produced or cached data. If the in-situ query is received by the sinks, the sink may answer it after fetching appropriate data from the farm server or its local cache. In the case of direct queries nodes forward the answers to the queries only when the answer was based on the data which is newer than in the case of answers already forwarded.

VI. SECURITY

This section discusses possible security threats to the target cattle monitoring system including unauthorized retrieval, modification and generation of data, as well as denial of service attacks (DoS). We propose ways how the security of the system can be improved and describe how the improved security affects the energy efficiency of animal mounted devices.

Due to the nature of cattle monitoring these solutions employ wireless sensor and mobile ad-hoc networks. They are therefore open to the all types of attacks typical for wireless networks and mobile ad-hoc networks as shown in Table 1.

Farmers who are owners of the system are likely to modify or fabricate data to put their products ahead of competition. They are also likely to suppress the data collection and event detection process, i.e., perform denial of service (DOS) attacks, in order to hide information such as spread of animal diseases.

They are most likely to target data collection process as they have unrestricted and unmonitored access to their animals and sensing equipment. Methods can involve taking animals out of range, temporary or permanently, so that their sensors can not send data to farm servers, refraining from changing batteries or changing data directly on farm servers. They can also perform DOS attacks that would globally disable the functionality of the system during the spread of animal disease. This involves physical layer attacks such as radio jamming.

Protecting the system against its potential owners may be risky because they may assume that introducing the system is against their business and thus they can be reluctant to that. Therefore, we do not consider this in a greater detail within this paper. The possible approach for creating incentives of such security against the owners' tampering would be granting quality certificates to the farmers who decide to adopt it. Potentially a greater awareness of security issues from farmers, retailers and consumers would be required for this model to be realistic.

Farm workers may want to tamper with the collected data to hide from management their misconduct - e.g., leaving animals on a pasture for too long or not providing them with water. This tampering will involve changing the collected data already stored on the farm servers. This form of attack can be avoided by appropriate securing the access to the databases storing this data, which is outside the scope of this paper.

Competitors are likely to disrupt functioning of the target farming enterprise or put it into a less favorable position. They are likely to modify or fabricate the data, as well as perform various DOS attacks. They will perform attacks on physical layer (e.g., radio jamming) or network layer. The latter involves deploying hostile nodes or modifying existing nodes in order to make them send incorrect route request or route reply messages in order to disrupt data delivery to sinks, answering in-situ queries or cause faster battery depletion. The hostile nodes can also send fabricated data or modify forwarded data to disrupt working of the farm. The precautions against these attacks are easier to introduce because owners of the system have strong incentives to support it. These attacks can be prevented by utilization of cryptographic primitives to encrypt and authenticate the exchanged data [34], which can increase energy consumption due to higher computational complexity and increased data traffic. Using cryptography in many cases requires public key infrastructure (PKI), which bares the infrastructureless mode that is otherwise feasible to our system. In the infrastructureless mode the sinks and farm servers are not deployed and users can only access the measurements via in-situ queries. The deployment of hostile or modified nodes can be detected by authentication of nodes via cooperative appraisal [35], that is a new approach to

security within wireless MANETs, which still has problems with disconnections and lower densities of topologies. Whenever a hostile node is detected, it can be isolated within the network (i.e., excluded from further communication) and its existence and approximate location can be communicated to the farm personnel.

Another intrusion detection technique for MANETs is based on anomaly detection [36]. More precisely nodes monitor network traffic generated by their neighbors and whenever deviation from the expected pattern is detected, the intrusion is assumed. In the animal monitoring this approach can potentially lead to a high number of false positive alerts. In particular unusual network activity can be caused by unexpected behavior of animals caused by fear, disease etc.

Another stakeholder, who may want to attack the cattle monitoring system are buyers of the animal products (e.g., supermarkets), who may want to lower the price of the products they buy or gather intelligence about the sellers to better evaluate their offer. Similarly as competitors they can perform DOS attacks, as well as modification or fabrication of data. They can also get unauthorized access to data by deploying passive nodes that would perform overhearing or active nodes that would forward the data and collect it. Passive overhearing can be only addressed by encryption of the exchanged data. Deployment of active spying nodes can be prevented by encrypting data or cooperative appraisal [35].

To summarize, there are numerous security threats against the proposed cattle monitoring system. Main feasible precautions include encryption, cryptographic authentication and cooperative anomaly detection – all of them are expensive in terms of processing and network traffic. Moreover, cryptographic methods typically requires infrastructure, which increases management costs.

VII. Conclusions and Future Work

In this paper, we discussed the practical deployment of the cattle monitoring system based on the mobile ad hoc disruption tolerant networking. Our extended field experiments justified the feasibility of such approach. We addressed the challenges posed by the real large scale deployment. More precisely we proposed the energy efficient approach for dealing with disconnections and discussed potential security threats and precautions. Our future work will further explore self organized infrastructures security models for the cattle monitoring.

Acknowledgements

The authors would like to thank the members of the School of Biosciences for their help and support in performing field experiments presented in Section 4.

References

[1] P. Zhang, C. M. Sadler, S. A. Lyon, and M. Martonosi, "Hardware Design Experiences in ZebraNet", In *Proc. of SenSys*, Baltimore, Maryland, USA, 2004.

[2] K. Mayer, K. Ellis, and K. Taylor, "Cattle Health Monitoring Using Wireless Sensor Networks", In *Proc. of CCN*, Cambridge, Massachusetts, USA, 2004.

[3] Z. Butler, P. Corke, R. Peterson, and D. Rus, "Dynamic Virtual fences for Controlling Cows", In *Proc. of ISER*, Marina Mandarin Hotel, Singapore, 2004.

[4] T. Wark, et al., "Transforming Agriculture through Pervasive Wireless Sensor Networks", *Pervasive Computing, IEEE*, April-June 2007, 6 (2), pp. 50-57.

[5] P. Corke and P. Sikka, "Results from the Farm", In *Proc. of EmNets*, Harvard University, Cambridge, MA, USA, 2006.

[6] T. Wark, et al., "The design and evaluation of a mobile sensor/actuator network for autonomous animal control", In *Proc. of International Conference on Information Processing In Sensor Networks (IPSN)*, Cambridge, Massachusetts, USA, 2007, pp. 206-215.

[7] B. Wietrzyk, M. Radenkovic, and I. Kostadinov, "Practical MANETs for Pervasive Cattle Monitoring", In *Proc. of the Seventh International Conference on Networking*, Cancun, Mexico, 2008.

[8] M. Radenkovic and T. Lodge, "Engaging the public through mass-scale multimedia networks", *IEEE Multimedia*, 2006, 13 (3), pp. 12-15.

[9] K. Maatje, R. M. d. Mol, and W. Rossing, "Cow status monitoring (health and oestrus) using detection sensors", *Computers and Electronics in Agriculture*, 1997, 16 (3), pp. 245-254(10).

[10] "HeatWatch® Estrus Detection System", CowChips, LLC, Available: http://www.heatwatch.com/. [May 17, 2009]

[11] A. Chaintreau, et al., "Pocket Switched Networks: Real-world mobility and its consequences for opportunistic forwarding", Computer Laboratory, University of Cambridge, Cambridge, UK, Technical Report 617, 2005.

[12] B. Wietrzyk and M. Radenkovic, "Energy Efficiency in the Mobile Ad Hoc Networking Approach to Monitoring Farm Animals", In *Proc. of the Sixth International Conference on Networking*, Sainte-Luce, Martinique, 2007.

[13] B. Wietrzyk and M. Radenkovic, "CRAWDAD data set nottingham/cattle", Available: http://www.crawdad.org/nottingham/cattle. [May 17, 2009]

[14] B. Krishnamachari, D. Estrin, and S. Wicker, "The impact of data aggregation in wireless sensor networks", In *Proc. of ICDCS*, 2002, pp. 575-578.

[15] R. Szewczyk, J. Polastre, A. Mainwaring, and D. Culler, "Lessons from a Sensor Network Expedition", In *Proc. of EWSN*, 2004.

[16] R. E. Kenward, *A Manual for Wildlife Radio Tagging*, Academic Press, 2001.

[17] T. Small and Z. J. Haas, "The shared wireless infostation model: a new ad hoc networking paradigm (or where there is a whale, there is a way)", In *Proc. of MobiHoc*, Annapolis, Maryland, USA, 2003.

[18] T. Small, Z. J. Haas, A. Purgue, and K. Fristrup, "A Sensor Network for Biological Data Acquisition", *Handbook on Sensor Networks*, 2004.

[19] Z. J. Hass and T. Small, "A New Networking Model for Biological Applications of Ad Hoc Sensor Networks".

[20] A. L. Iacono and C. Rose, "Infostations: New Perspectives on Wireless Data Network", in *Next Generation Wireless Networks*, vol. 598: Springer Netherlands, 2002, pp. 3-63.

[21] D. J. Goodman, J. Borras, N. B. Mandayam, and R. D. Yates, "INFOSTATIONS: a new system model for data and messaging services", In *Proc. of Vehicular Technology Conference*, Phoenix, AZ, USA, 1997, pp. 969-973.

[22] Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-based ad hoc routing", *IEEE/ACM Trans. Netw.*, 2006, 14 (3), pp. 479-491.

[23] M. Demmer and K. Fall, "DTLSR: delay tolerant routing for developing regions", In *Proc. of Applications, Technologies, Architectures, and Protocols for Computer Communication*, Kyoto, Japan, 2007.

[24] A. Lindgren, A. Doria, J. Lindblom, and M. Ek, "Networking in the land of northern lights: two years of experiences from DTN system deployments", In *Proc. of International Conference on Mobile Computing and Networking*, San Francisco, California, USA 2008.

[25] A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, "Low-cost communication for rural internet kiosks using mechanical backhaul", In *Proc. of International Conference on Mobile Computing and Networking*, Los Angeles, CA, USA 2006, pp. 334 - 345.
[26] X. Zhang, J. Kurose, B. N. Levine, D. Towsley, and H. Zhang, "Study of a bus-based disruption-tolerant network: mobility modeling and impact on routing", In *Proc. of International Conference on Mobile Computing and Networking*, Montréal, Québec, Canada, 2007, pp. 195 - 206.
[27] M. Radenkovic and B. Wietrzyk, "Mobile Ad Hoc Networking Approach to Detecting and Querying Events Related to Farm Animals", In *Proc. of ICNS*, Santa Clara, California, USA, 2006, pp. 109-115.
[28] C. J. C. Phillips, *Principles of cattle production*, CABI Publishing, Oxon, UK, 2001.
[29] E. J. Riedy and R. Szewczyk, "Power and Control in Networked Sensors", 2000.
[30] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks": Kluwer Academic, 1996.
[31] M. Tarique, K. E. Tepe, and M. Naserian, "Energy Saving Dynamic Source Routing for Ad HocWireless Networks", In *Proc. of WIOPT*, 2005.
[32] M. R. Gosnell, R. Albarelli, M. X. Cheng, and B. McMillin, "Energy Balanced Broadcasting Through Delayed Intelligence", In *Proc. of ITCC*, 2005, pp. 627-632.
[33] M. Radenkovic and B. Wietrzyk, "Wireless mobile ad-hoc sensor networks for very large scale cattle monitoring", In *Proc. of ASWN*, Berlin, Germany, 2006, pp. 47-58.
[34] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", In *Proc. of WiSe*, Atlanta, Giorgia, USA, 2002.
[35] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: self-organized network-layer security in mobile ad hoc networks", *IEEE Jurnal on Selected Areas in Communications*, 2006, 24 (2), pp. 261-273.
[36] Y.-a. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks", In *Proc. of 1st ACM workshop on Security of ad hoc and sensor networks*, Fairfax, Virginia, 2003, pp. 135-147.

TABLE I. POTENTIAL ATTACKERS

Location\Attacker	**Owners**	**Competitors, buyers**
Individual animal being monitored, monitoring hardware	Tampering with monitoring hardware, removing or disabling sensors to change sensed data	
Radio waves communication (physical layers)	Signal jamming, moving devices or animals out of network coverage.	Signal jamming, modification and fabrication of data by deploying malicious devices or modifying existing devices
Link Layer		Illegitimate access and fabricating or modifying data
Network Layer		Illegitimate access and fabricating or modifying data, routing attacks