CEAS 2009 European Air and Space Conference (ISBN 1 85768 208 4), 26 -29 October 2009, Manchester, UK

Efficient Communication in Self-organizing Mobile Sensor (Ad-Hoc) Nets - Mathematical Foundation, Algorithmization, Simulation

Peter H. Richter
O & S Consultancy

In this paper an advanced MANET algorithm / protocol is given based on a graph theoretical approach. We start with a general mathematical / graph theoretical analysis of the universal instance and problem in order to state a traceable objective function for the optimization. Afterwards we give an efficient and optimal solution algorithm that (a) ..neither uses geographic specifications nor assumes that the sensor nodes are quite stationary, (b) ..globally works as a shortest path algorithm although no path information is stored in an information center or server, (c) ..makes available the best forward / backward tracing of queries / answers such that no better path between sources and targets can be found for the actual volatile situation, (d) ..eliminates straying messages as soon as possible meeting the broadcast storm problem, (e) .. has the least system overhead conceivable and the least negotiation protocol.

1. Introduction

Mobile ad hoc networks (MANETs) are collections of autonomous mobile sensors (we say here ‘nodes’) changing messages via wireless connections. MANETs are expected to play an essential role in future military and civilian applications, where no communication infrastructure does exist or should be used.

This paper is concerned with the design of a routing layer, i.e. a messaging algorithm (implemented into all net nodes) and a corresponding protocol. Because the nodes are assumed to be mobile, unpredictable traffic patterns and changing network topologies are to take into consideration. Existing wireless algorithms and protocols are insufficient primarily as to the consideration of the mobility and power requirements of clients and servers – an essential issue because many MANETs are assumed battery powered.

Thus, the proposed **s**ensor **n**etwork **r**outing algorithm **A-SNR** given below has to work in a self-organizing and very energy-efficient manner (small algorithms, small protocol). Despite a spatial changing of the nodes’ position or even the drop out of some nodes the message-traffic remains sustainable as long as at least one connection path via intermediary nodes does exist for a demanded source – sink inquiry. A straightforward broadcasting by flooding is usually very costly resulting in serious redundancy, and collision, called broadcast storm problem. Algorithm **A-SNR** enables a message routing being as irredundant as possible with respect to the proposed message protocol and to meet the broadcast storm problem. Security matters and the different sparse distribution of sensors within a regarded spatial environment area can made it necessary that several sources have simultaneously to send the same inquiry with the same global unique identifier GUI id to several other targets (Distributed Multicast). **A-SNR** takes this into consideration and enables that each reachable node accepts and passes the first receiving id-message only once. The encountered targets, so far demanded by the inquiring messages, send back the required data to all sources in similar manner without using the paths over which the messages came from what is in the interest of the MANET’s robustness.

1.1 Related Works

- Tan He et al. [7] proposed an aggregation scheme that adaptively and time sensitively performs application-independent data aggregation. The method isolates aggregation decisions into a module that resides between the network and the data-link layer and doesn’t require any modifications to the currently existing MAC and network layer protocols (novel adaptive feedback scheme). It is shown that that end-to-end transmission delay is reduced by as much as 80 %; under heavy traffic loads, and that as much as a 50 % reduction in transmission energy consumption occurs with an overall reduction in header overhead.
- Padmanabhan et al.[16] identified issues involved in MANET data replication and attempts to classify existing MANET data replication techniques based on the issues they address. The attributes of the replication techniques are tabulated to facilitate a feature comparison of the existing MANET data replication works. Parameters and performance metrics are presented to measure the performance of MANET replication techniques.
- Yu-Chee Tseng et al. [18] identified the broadcast storm problem by showing how serious it is through analyses and simulations. They proposed several schemes to reduce redundant rebroadcasts and differentiate timing of rebroadcasts. Simulation results are presented.
- Gopalakrishnan et al. [5] regard the scalability analysis of MANETs and describe approaches to speeding up the M&S phase while analyzing MANETs. They propose techniques analyzing the scalability performance of a dynamic policy-based network management system.
- Kyu-Hwan Lee et al. [15] proposes an ad hoc authentication protocol for home environments implemented into the ad hoc routing algorithm. The analysis shows that the proposed protocol provides a secure home network environment without significant performance degradation.
- Chi-Fu Huang et al. [10] proposed a two-tier, heterogeneous MANET architecture supporting Internet access. The low tier consists of a set of mobile hosts each equipped with a IEEE 802.11 card. In order to connect to the Internet and handle the network parti-

tioning problem, it has been proposed the high tier consisting of a subset of the mobile hosts (gateways), accessing the cellular/infrastructure networks. The network interfaces in the gateway hosts could be IEEE 802.11 cards, PHS handsets, or GPRS handsets. To avoid gateway bottlenecks and to solve the load-balance routing issue a set of solutions (boundary-moving, host-partitioning, and probabilistic solutions) has been proposed.

Qunwei Zheng et al. [19] regard recent advances in mobility modeling MANET research: some new mobility models and analysis of older models classifying the models into three categories according to the degree of randomness while introducing newly proposed models in each of these categories.

- El-Bazzal et al. [3] propose a clustering algorithm 'Efficient Management Algorithm for Clustering' (EMAC) based on weighting parameters to reduce the number of clusters, maintaining stable clusters, minimizing the number of invocations for the algorithm and maximizing lifetime of mobile nodes. Through simulations the authors compared the performance of their algorithm with that of WCA in terms of the number of clusters formed and number of states transitions on each cluster head. The results demonstrate the superior performance of the proposed algorithm.
- Leslie D. Fife et al. [4] discuss issues associated with data communication with MANET database systems. While data push / pull methods have been previously addressed in mobile networks, they do not handle the requirements associated with MANET: Unlike traditional mobile networks, all nodes within the MANET are mobile and battery powered. Existing wireless algorithms and protocols do not consider sufficiently enough the mobility and power requirements of clients and servers. The paper presents some of the critical tasks facing this research.

1.2 Notation / Specification

In order to be able to grasp the algorithms detailed functioning we rely on the concepts of analysis and graph description language.

P is the set of "sensors" or "nodes" and denotes the set of mobile communicating entities (versatile entities equipped with sensors):

$\mathbf{S} \subset P$ is the set of source nodes (shortly sources) functioning as inspection nodes or control stations for observations and maintenance of other nodes.

$\mathbf{T} \subset P$ is the set of destination nodes (shortly targets) being entities to be inspected, controlled, inquired, .., $|T| \geq 1$, $S \cap T = 0$.

$\hat{\mathbf{T}} \subseteq T$ denotes those targets that are accessible from at least one source $s \in S$ with respect to **G** and ψ_{min} (see below).

$\breve{\mathbf{T}} \subseteq \hat{\mathbf{T}} \subseteq T$ denotes those targets that have reached a reply demand (contained within the μ-message).

ψ: $P \times P \rightarrow \boldsymbol{R}_+$ [1], called signal strength.

$\psi(p, q)$ is the current signal strength of a message at q coming from p.

ψ_{min} denotes the minimum signal strength acceptable for a faultless messaging between two nodes.

$\psi(p, q) < \psi_{min} \Rightarrow$ A faultless transmission from p to q is assumed to be not possible.

$\mathbf{G} = [V_\mathbf{G}, E_\mathbf{G}] = [P, R]$ is called dynamic ubiquity graph or net domain consisting of certain ordered pair of graph vertices $V_\mathbf{G} = P$ and graph edges $E_\mathbf{G} = R$ with $R \subseteq P^2$ as follows:

$R = \{(p, q) \in P \times P: \psi(p, q) \geq \psi_{min}\}$.

The set of edges R increases or decreases dependent nodes' mobility and therefore on the signal strength $\psi(p, q) > \psi_{min}$ between p and q, i.e. a certain layout of **G** may yield only for a short moment. The communication concept described below starts from the assumption that the nodes are changing their position (e.g. like cars in a traffic environment), i.e. the concept **G** takes into account the volatility of **G**.

$\mathbf{G'} = [\mathbf{V}_{G'}, E_{\mathbf{G'}}]$ is called a sub-graph $G' \subseteq G$, if $\mathbf{V}_{G'} \subseteq V_G$ and $E_{\mathbf{G'}} \subseteq E_G \cap \mathbf{V}_{G'}^2$.

$\xi = R^o \subseteq V_G^2$ is called "accessibility" [2]. It is the reflexive, symmetric and transitive closure of the edges $R = E_G$. We write $(p, q) \in \xi$ or shortly $p\xi q$ if node q is reachable from node p and vice versa in the current net **G** observing ψ_{min}.

Accessibility ξ depends on the mobility of P what influences the deletion and creation of the graph edges R (changed topology of **G** and therefore ψ).

η: $V_G \rightarrow \boldsymbol{R}_+$ denotes the vertex cost as node deceleration time / latency. If one message passes vertex p then $\eta(p) > 0$ decelerates forwarding the incoming message. As a first pragmatic approach for the simulation we take

$$p \in P \Rightarrow \eta(p) = c_1 \in \boldsymbol{R}_+ \tag{1.1}$$

λ: $R \rightarrow \boldsymbol{R}_+$, denotes the edge cost as direct transduction time. Let $p\xi q$ (i.e. $\psi((p,q)) \geq \psi_{min}$). As a convenient approach for the simulation we take

$$\lambda(e) = c_2 \in \boldsymbol{R}_+. \tag{1.2}$$

C(G'**)** denotes the cost of a sub-graph $G' \subseteq G$ with

$$C(G') = \underbrace{\sum_{v \in V_{G'}} \eta(v)}_{\text{vertex cost}} + \underbrace{\sum_{e \in E_{G'}} \lambda(e)}_{\substack{\text{insignificant} \\ \text{edge cost}}} . \tag{1.3}$$

$\mathbf{P}_G(p, q) \subseteq \mathbf{G}$ describes an optimal transmission path from $p \in P$ to $q \in P$. $\mathbf{P}_G(p, q)$ is a sub-graph in **G** observing ψ_{min} such that its evaluation $C(\mathbf{P}_G(p, q))$ is minimal with respect to the transmission cost:

---

[1] ***R*** represents the set of all ***Real Numbers***, $\boldsymbol{R}_+$ is the set of positive real numbers. ***N*** is the set of ***Natural Numbers***.

[2] $\xi = R^\circ \supseteq R \subseteq P \times P$ as follows:
ξ reflexive: $p \in P \Rightarrow (p, p) \in \xi$
ξ symmetric: $(p, q) \in \xi \Rightarrow (q, p) \in \xi$
ξ transitive: $(p, q) \in \xi \wedge (q, r) \in \xi \Rightarrow (q, r) \in \xi$

$$C(\mathbf{P}_G(p, q)) = \min_{\substack{\mathbf{P}'\subseteq \mathbf{G}\\ p\xi q}} \{C(P')\}. \qquad (1.4)$$

(1) $p\xi q \Rightarrow \mathbf{P}_G(p, q)$ exists with cost $C(\mathbf{P}_G(p, q))$.

(2) $\neg\, p\xi q \Rightarrow \mathbf{P}_G(p, q)$ [3] doesn't exist.

2. Data Basis

2.1 Message Records

$\mu = (\mathbf{1}, id, s, T, \alpha)$

Message μ coming from all source $s\in S$ with GUI [4] id is intended to transmit information content $\alpha\in\Sigma^*$ containing inquiries or control commands to all the targets T (intended to be reached).

If $|S| > 1$ (Distributed Multicast), all $s\in S$ simultaneously fire a μ with the same id. In this case the message contents have to be the same! Each node $p\in P$ accessible from its "nearest" source $s\in S$ accepts a μ-message with a specific id only once! This means that all μ-messages with the same id arriving later are rejected (not processed) by p.

Parameter α may contain <u>inquiries</u> for the targets' state variables or environment data . Then the corresponding answers (τ-answers below) have to be sent back from all $t\in T$ to all sources $s\in S$.

$\tau = (\mathbf{2}, id, t, \beta(t,\alpha))$

Response τ is an answer-message coming from a target $t\in T$ that has received a μ-message with GUI id that is the same id as contained in the inquiring $\mu = (\mathbf{1}, id, s, T, \alpha)$. τ is being only launched by t if an answer $\beta(t, \alpha) \in \Sigma^*$ is demanded by μ (here simply assumed to be encrypted in α). Otherwise, a τ-message is not fired. Each node $p\in P$ accepts a τ-message containing the tuple (id, t) only once! This means that all τ, arriving p later with the same tuple (id, t), are rejected by p.

2.2 Broadcast State Records

μ and τ are also used as state records stored by the nodes $p\in P$ so far they fire or get a μ or get a τ-message. We derive the state records from the message records described in 2.1:

$\mathbf{\Omega_1}$ and $\mathbf{\Omega_2}$ are a finite sets of state records stored in each node $p\in P$.

$\mathbf{\Omega_1} = \{$(id, s), ((id', s'), …. $\Leftrightarrow$ μ-contents

Each ordered set (id, s) $\in \Omega_1$ indicates that p has already faultlessly received a μ-message with GUI id. Then, node p is indebted not to accept again a μ with the same id. If a second message μ with the same id arrives p again no action occurs, i.e. this second message (like other μ-messages with the same id coming afterwards) is not processed and forwarded. A record containing parameter $s \neq 0$ means that node $p\in S$ (as a source) has created and fired a μ-message. $s= 0$ means that node p has received and fired μ-message.

$\mathbf{\Omega_2} = \{$(id, t), (id', t'), ….$\}$ $\Leftrightarrow$ τ -contents.

Each ordered set (id, t) $\in \Omega_2$ indicates that node p containing this record has already faultlessly received and forwarded a τ-message with GUI id from target t. Then, node p is indebted not to accept again a τ with the same id and t afterwards. If a second τ with the same id and t arrives p again no action occurs.

3. Problem Formulation Optimal Self-organizing Sensor Net

3.1 Inquiry-messaging: "μ-messaging"

3.1.1 Definitions

$f: P \rightarrow S$ called <u>target - source assignment</u> is a single-valued partial function that inherently emerges from the accessibility $\xi = R^{o}$

(1) $f(p) = s\in S$:

$$s\xi p \;\wedge\; C(\mathbf{P}_G(s, p)) = \min_{s'\in S} \{C(\mathbf{P}_G(s', p))\}.$$

$f(p)$ assigns p the nearest source $s\in S$ from which p is accessible.

(2) $f(p) = \perp$ (not defined) if $\forall s\in S: [\neg\, s\xi p\,] \approx$ "p not accessible" from any $s\in S$.
For this case we define $C(\mathbf{P}_G(s, p)) = \infty$.

$\hat{\mathbf{T}} \subseteq T$ is the set of accessible destinations:

$$\hat{\mathbf{T}} = \{t\in T: \Leftrightarrow \exists s\in S:[s\xi t]\} = \{t\in T: f(t) \in S\}.$$

3.1.2 Problem "μ -messaging"

<u>Given</u>: Instance as to 3.1, sources S, targets T.

<u>Problem</u>: Determine a communication graph $\mathbf{H} \subseteq \mathbf{G}$ such that each accessible $t\in T$ receives its μ-message via an optimal, robust and irredundant connection from one (and only one) source $f(t)\in S$.

<u>Task</u>: Find a μ-messaging algorithm implemented in each node $p\in P$ such that the messaging traffic results to an optimal communication net $\mathbf{H} \subseteq \mathbf{G}$ working as efficient as possible.

<u>Solution Domain</u>:

Dependent on $\mathbf{G}$, $\mathbf{H}$ consists of $|S|$ several disjoint subgraphs $\mathbf{H}_s$ each rooted at $s\in S$ as follows:

(a) $s\in f(\hat{\mathbf{T}}) \Rightarrow$ at least one $t\in T$ is accessible from s:

$$\mathbf{H}_s = \bigcup_{\forall t\in f^{-1}(s)} \{P_G(s,t)\}. \qquad (1.6)$$

$\mathbf{H}_s$ is a communication tree rooting at s.

(b) $s\notin f(\hat{\mathbf{T}}) \Rightarrow$ s cannot access any $t\in \hat{\mathbf{T}} \Rightarrow$
$\mathbf{H}_s = [\{s\}, 0]$ is called singleton.

(c) $t\in \mathbf{T} \;\wedge\; f(t) = \perp$ ("not defined") $\Rightarrow$
$t\in T$ is not accessible from any $s\in S$.

Now, the <u>μ-communication graph</u> results to

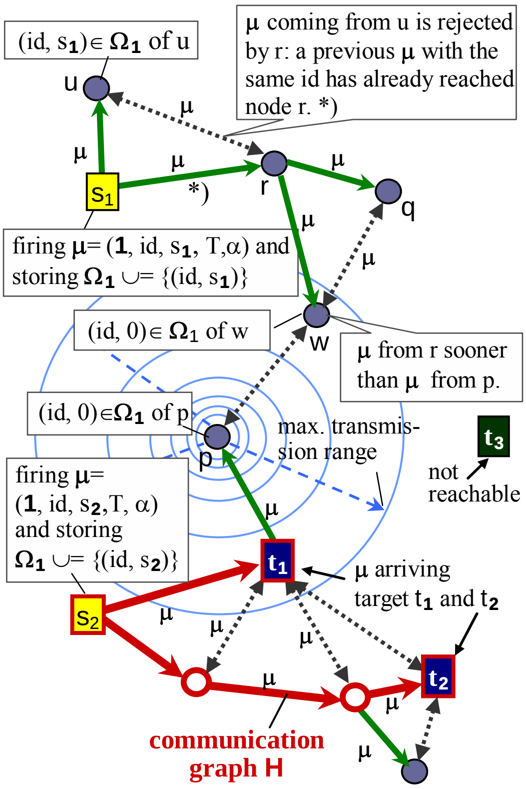
$$\mathbf{H} = \bigcup_{\forall t\in\hat{T}} P_G(f(t), t) = \bigcup_{\forall s\in f(\hat{T})} H_s . \qquad (1.7)$$

---

[3] $\neg\, p\xi q$ = "q not accessible from p".

[4] GUI - Global Unique Identifier

H is the set of $|f(\hat{\mathbf{T}})|$ disjoint communication trees H_S and consists of $|\hat{\mathbf{T}}| = |f^{-1}(S)|$ optimal transmission paths $\{\mathbf{P}_G(f(t), t)\text{: } t\in \hat{\mathbf{T}}\}$.



*) $C(\mathbf{P}_G(s_1, r)) < C(\mathbf{P}_G(s_1, u)) + C(\mathbf{P}_G(u, r))$.

Fig. 1 Example for a μ-messaging in G

$S = \{s_1, s_2\}$, $T = \{t_1, t_2, t_3\}$,

accepted messages μ 🟩→ and 🟥→,

rejected messages μ ⋯→,

Target $t_3 \in T$ is not accessible, $\hat{\mathbf{T}} = \{t_1, t_2\}$,

$f(t_1) = f(t_2) = s_2$, source s_1 cannot access any target.

Communication graph $H = \bigcup_{\forall s\in f(\hat{T})} H_S =$ 🟥→.

3.2 Response-messaging: “τ-messaging”

3.2.1 Definitions

$\breve{\mathbf{T}} \subseteq \hat{\mathbf{T}} \subseteq T$ is the set of accessible targets in $\hat{\mathbf{T}}$ that are required to respond to the calling sources **S**.

$\breve{\mathbf{T}} = \{t\in \hat{\mathbf{T}} : t \text{ got a } \mu \text{ from } f(t) \text{ requiring a reply}\}$.

In contrast to the μ -messaging that sends inquiries to the targets, the τ-messaging sends responses from the targets to the inquiring sources so far demanded by α in μ. The μ-messaging runs such that several sources might simultaneously send the same inquiry to several other targets (see Fig. 2). The τ-messaging leads to another communication graph $\bar{H}$ different to H. Each source $t\in \breve{\mathbf{T}}$ demanded to send back an answer to the calling sources of S might have its own specific response β(t,α) derived from the corresponding data stock of node t.

3.2.2 Problem “τ -messaging”

Given: Instance as to 3.2, sources S, targets $\breve{\mathbf{T}}$.

Problem: Determine a communication graph $\bar{\mathbf{H}} \subseteq \mathbf{G}$ such that each accessible $s\in S$ receives its τ-message via an optimal, robust and irredundant connection from all $t\in \breve{\mathbf{T}}$.

Task: Find a τ-messaging algorithm implemented in each node $p\in P$ such that the messaging traffic results to an optimal communication net $\bar{\mathbf{H}} \subseteq \mathbf{G}$ working as efficient as possible.

Solution Domain:

Dependent on **G**, $\bar{H}$ consists of $|\breve{\mathbf{T}}|$ non-disjoint sub-graphs $\bar{\mathbf{H}}_t$ each rooted at $t\in \breve{\mathbf{T}}$ as follows:

(a) $t\in \breve{\mathbf{T}} \wedge \forall s\in S$:

$$\bar{\mathbf{H}}_t = \bigcup_{\forall s\in S} \{\mathbf{P}_G(t, s)\} \text{ is a tree rooting at t.} \tag{1.8}$$

(b) $t\in \breve{\mathbf{T}} \wedge \forall s\in S\text{: } [(t, s) \notin \xi] \Rightarrow$ t cannot answer to any source $s\in S$. $\bar{\mathbf{H}}_t = [\{t\}, 0]$ is a singleton.

(c) $s\in S \wedge \forall t\in \breve{\mathbf{T}}\text{: } [(t, s) \notin \xi] \Rightarrow s\in S$ is not accessible from any $t\in \breve{\mathbf{T}}$.

Now, the τ-communication graph results to

$$\bar{\mathbf{H}} = \bigcup_{\forall (t,s)\in \breve{T}\times S} \{\mathbf{P}_G(t, s)\} = \bigcup_{\forall t\in \breve{T}} \bar{H}_t\ . \tag{1.9}$$

$\bar{\mathbf{H}}$ is the set of non-disjoint sub-graphs rooted at all $t\in \breve{\mathbf{T}}$. $\bar{\mathbf{H}}$ consists of at most $|\breve{\mathbf{T}}|\cdot |S|$ paths.

The presented algorithm **A-SNR** is intended to be implemented in each node $p\in P$.

4. Solution Method

4.1 Posting Inquiries: **μ-messaging**

Several sources $S \subseteq P$ address the same set of targets $T \subseteq P$ to send them a μ-query $(\mathbf{1}, id, s, T, \alpha)$. Each node $p\in P$ that receives a μ with this id for the very first time stores this μ-message as state record only once. Further μ-messages with the same id arriving p later are rejected by p.

Fig. 1 reveals that this proceeding leads to a structure called forest $\mathbf{H} = \bigcup_{\forall s\in f(\hat{T})} H_S$ of optimal path trees $\mathbf{H}_S$, although **H** (in Fig. 1) consists of only one tree. Source s_1 cannot reach any target $t\in \hat{\mathbf{T}}$.

Lemma 1

If all sources $s\in S$ coevally fire a μ-query with the same GUI id and if each node $p\in P$ is programmed such that it accepts, stores and forwards an incoming query μ with the same id only once, then the whole spreading μ-messaging self-organizes an optimal communication graph $\mathbf{H} \subseteq \mathbf{G}$.

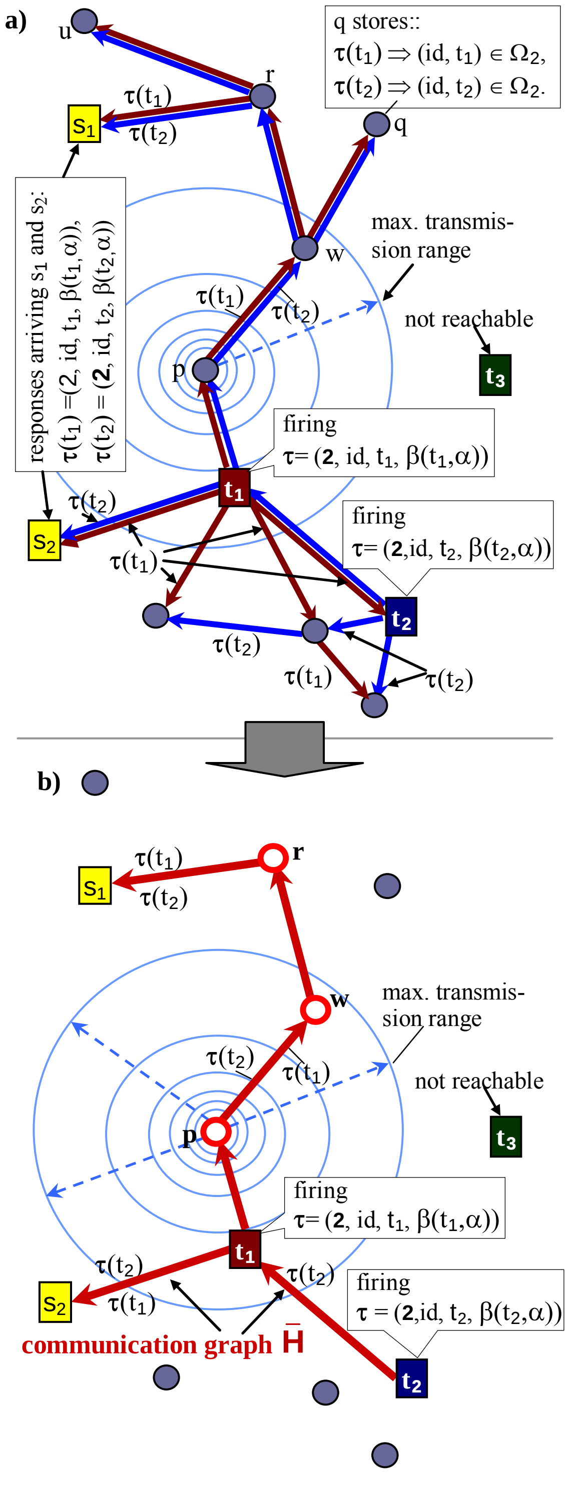


Fig. 2 A τ-messaging after a μ-inquiry of Fig. 1:
$S= \{s_1, s_2\}$, $T= \{t_1, t_2, t_3\}$, $\hat{\mathbf{T}}=\{t_1, t_2\}$, accepted messages τ: → and →,
$\bar{\mathbf{H}}_{t_1} =$ →, and $\bar{\mathbf{H}}_{t_2} =$ →, $\bar{\mathbf{H}} = \bigcup_{t\in\hat{T}} \bar{H}_t =$ →.

Proof

We only have to show, that each p∈ P receives μ via an optimal path $\mathbf{P}_G(s, p)$ from s to p in **G** so far sξp.

1. We regard a special p∈ P that receives one message μ for the very first time. This μ comes from a specific s∈S. We assume, that μ hasn't used an optimal path $\mathbf{P}_G(s, p)$ in **G** but a path $\mathbf{P}'_G(s, p)$ that also observes sξp. A better path must have enabled μ to reach p earlier than using $\mathbf{P}_G(s, p)$. This contradicts the assumption that **P**'(s, p) is a better path than $\mathbf{P}_G(s, p)$.
2. We regard some node p∈P that coevally receives several messages $M_{id}=\{\mu_1, \mu_1, .., \mu_n\}$ with the same id coming from different intermediary nodes (transmitters).
   (a) p has already received a μ-message earlier. Then, a $\mu_x \in M_{id}$ is blocked from processing. Corresponding to 1., the first μ came via an optimal path!
   (b) p hasn't received a μ with GUI id. Since all $\mu_x \in M_{id}$ arrive p coevally they came via equally well optimal paths what justifies selecting an arbitrary $\mu_x \in$ M. ■

Algorithm **A-SNR** observes Lemma 1, see Fig. 3.

4.2 Sending Answers: τ-messaging

The receiving nodes $t \in \hat{\mathbf{T}}$ decides (dependent on α in μ) whether the calling sources have to get an answer β(t, α) wrapped by a response message τ=(**2**, id, t, β(t,α)). If so, i.e. $t\in \breve{\mathbf{T}}$, τ is fired back by t intended to reach all the sources S. In contrast to the μ-messaging graph **H,** the τ-messaging corresponds to a set of generally non-disjoint trees $\bar{\mathbf{H}}_t$ each rooting at a target $t\in \breve{\mathbf{T}}$. A node p forwards a received τ-message only then if it hasn't yet stored a state record with the same tupelo (id, t) within τ.

Lemma 2

If each node p∈ P controls the incoming τ-messages such that only the first one with specific tupelo (id, t) is forwarded then a tree $\bar{\mathbf{H}}_t = \bigcup_{s\in S} \mathbf{P}_G(t,s)$ of optimal communication paths $\mathbf{P}_G(t,s)$ rooting in $t\in \breve{\mathbf{T}}$ will be built in **G** for that specific τ.

Proof

We refer to Lemma 1 because the proof for Lemma 2 is similarly to conduct as described in Lemma 1.

4.3 Solution Algorithm A-SNR

Fig. 3 describes the algorithm that is to implement in each node p∈ P that might function as source, target, or transponder. Ω_p established as queue contains the set of state variables of each node p. Each τ or μ pushed into Ω_p should be deleted after a well determined time dependent on the application in order to reduce storage space each node. D_p denotes the queue established in the current sources p=s∈ S (see Step 15 in Fig. 3) containing the answers (t, β(t, α)) coming from an answering target $t\in \breve{\mathbf{T}}$. Each tupelo (t, β(t,α)) contained in D_p should also be deleted by the receiving source after a certain time depending on the effort for analyzing (t, β(t, α)).

In the following we describe each step of the algorithm **A-SNR** corresponding to Fig. 3:

Algorithm **A-SNR** corresponding to **Fig. 3**

1 Preparing an inquiry μ in a source $s\in S$.

2 Firing the prepared inquiry **μ**. ↯.

3 Storing (id, s) as μ-state record of Ω_1.
End.

4 ↯ A μ arrives node $p\in P$.

5 If this μ has already reached node p before then
End.

6 Store (id, 0) as state record of Ω_1 expressing that μ hasn't been originally fired (in contrast to 3).

7 If this node $p\in P$ is not a target of **μ** go to **10**.

8 Determine the answer $\beta(p, \alpha)$ related to μ and fire answer τ ↯.

9 If p is the only target in T then
End.

10 Fire the received μ ↯ to further targets.
End.

11 ↯ A τ arrives node $p\in P$.

12 If this τ has already arrived $p\in P$ before then
End.

13 Store (id, t) into Ω_2.

14 Is τ an answer for this node $p\in P$ (i.e. is p a source that awaits this incoming τ)? If no then go to **16**.

15 Else, $p\in S$ has received a τ-answer for a previous μ-inquiry. The answer $\beta(t, \alpha)$ received from target t is to process.

16 Fire this τ towards further sources $s\in S$ ↯.

17 **End**.

4.4 Operation Modes

The following modes assume that all μ-messages require an answer from the accessible targets $\hat{\mathbf{T}}\subseteq T$, i.e. $\breve{\mathbf{T}}=\hat{\mathbf{T}}$.

4.4.1 Unicast

$S=\{s\}$, $\breve{\mathbf{T}}=T=\{t\}$.

- Straying μ-messages: $O(|P|)$.
  Each node $p\in P$ is restricted to forward only one μ with the same id.
- Straying τ-messages: $O(|P|)$.
  Each node $p\in P$ is restricted to forward only one τ-answer with the same id.

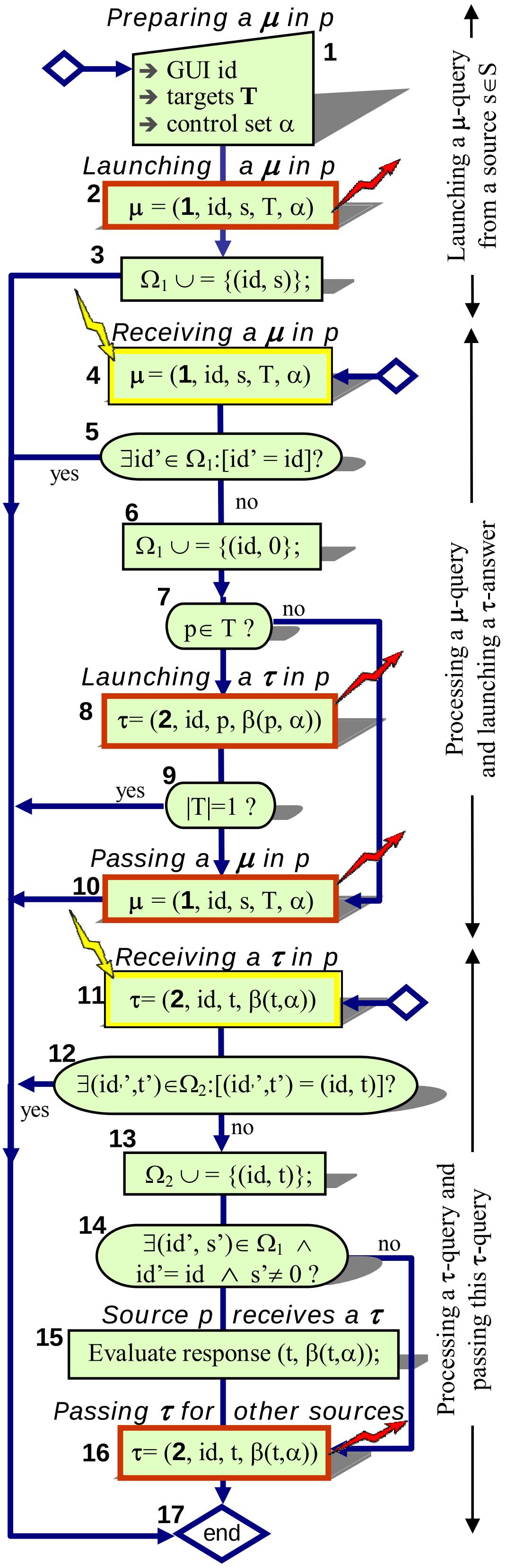


Fig. 3 Algorithm **A-SNR** established in each node $p\in P$ of the MANET.
$p\in P$ receives a message: ↯,
$p\in P$ fires a message: ↯.

4.4.2 Multicast

S= {s}; $\breve{\mathbf{T}} = \mathbf{T} \subseteq P$.

- Straying μ-messages: $O(|P|)$.
  Each node $p \in P$ is restricted to forward only one μ with the same id. A target $t \in \mathbf{T}$ receives and forwards also only once.
- Straying τ-messages: $O(|\breve{\mathbf{T}}| \cdot |P|)$.
  Each target $t \in \breve{\mathbf{T}}$ is expected to send its own τ= (**2**, id, t, β(t, α)) back to the inquiring source $s \in S$ Each node $p \in P$ is restricted to forward only one τ- answer with the same id.

Notice, each target fires back a different τ-message and each node $s \in P$ can store and forward totally $|\breve{\mathbf{T}}|$ different messages.

4.4.3 Distributed Multicast

|S| > 1; |T| > 1.

This mode is demanded for modern mission critical applications:

- Predefined sources S fire corresponding to predefined time adjustments μ-inquiries to predefined targets in order to get τ-answers from them considering that
- some targets may only be accessible from sources situated within some targets' vicinity.

Distributed Multicast is robust because it generally ensures a better accessibility so far the sources S are sufficiently distributed (signal range coverage) among the different clusters of the targets T. Note, because all the sources S fire the same μ-messages it is sufficient for all targets that they receive only one of these identical μ-messages regardless from which source $s \in S$ they should come!!

- Straying μ-messages: $O(|P|)$.
  Each node $p \in P \setminus S$ forwards a message with the same id only once.
- Straying τ-messages: $O(|\breve{\mathbf{T}}| \cdot |P|)$,
  as explained in Multicast.

In this context we only want to mention some further concepts:

4.4.4 Broadcast

is Multicast with $T = P \setminus \{s\}$.

4.4.4 Geocast

is in demand if a μ-inquiry is to address only those nodes that are situated within a certain geographic region. For this case, α in μ has to contain the corresponding geographic information and the sensors T= P have to be equipped with

(a) the fix geographic position (stationary sensors),
(b) the corresponding GPS facilities to provide the geographic position (mobile sensors).

5. Complexity and Simulation

5.1 Complexity

Lemma 3

Using algorithm **A-SNR**, the resulting MANET traffic for one GUI id in graph G needs a time effort

$$O(|\breve{\mathbf{T}}| \cdot |P|).$$

Proof:

Algorithm **A-SNR** is implemented in each of the nodes P. We regard one id-communication and assume

$t_{\mu p}$ as time needed to process μ in p and

$t_{\tau p}$ as time needed to process τ in p.

It follows corresponding to the operation mode **Multicast** and **Distributed Multicast**:

$$O\Big(\sum_{p \in P} t_{\mu p} + |\breve{\mathbf{T}}| \cdot \sum_{p \in P} t_{\tau p}\Big) = O(|\breve{\mathbf{T}}| \cdot |P|). \qquad \blacksquare$$

5.2 Simulation and Test

We generated random graphs **G**= [P, R] consisting of

- vertices $V_{\mathbf{G}} = P$ (nodes= sensors / transponders) $10^3 \le |P| \le 10^4$ with a cost function $\eta: V_{\mathbf{G}} \to \{1\}$ and
- edges $E_{\mathbf{G}} = R = \{(p, q) \in P^2 : d(p,q) \ge \psi_{\min}\}$ with cost function $\lambda: R \to \boldsymbol{R}_+$ as follows:

$$\begin{bmatrix} \psi(p,q) \ge \psi_{\min} & \Leftrightarrow & \lambda(p,q) = \psi(p,q) = d(p,q) \\ \text{else} & \Leftrightarrow & \text{edge } (p,q) \text{ doesn't exist} \end{bmatrix} \text{ with}$$

$d(p,q)$ as the Euclidean distance between p and $q \in P$ where $\psi_{\min}$ is related to a max. transmission distance $d_{\max}$ as to $\psi(p,q) \ge \psi_{\min} \Leftrightarrow d(p,q) \le d_{\max}$.

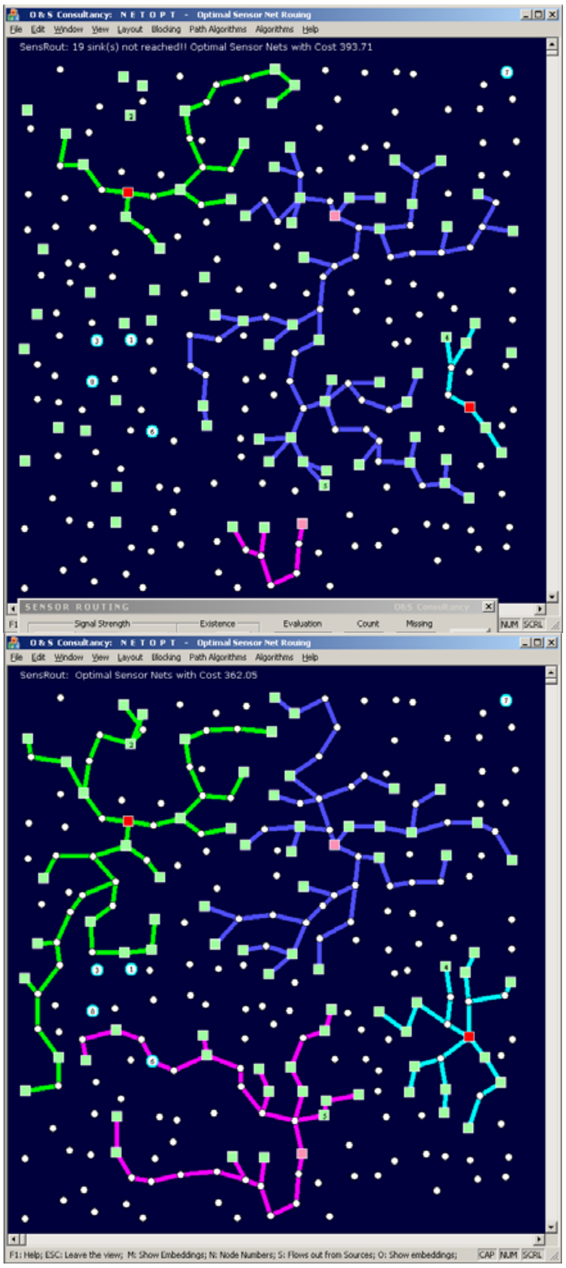
The tests have been run with the input **G**, S, T, where **G** has been generated as planar random graph with a predefined number of nodes P and the successive random assignment of $S, T \subseteq P$, see **Error! Reference source not found.**. A slight increase of $d_{\max}$ may change the appearance of communication graphs H and $\bar{\mathbf{H}}$ quite drastically.

Error! Reference source not found. shows two optimal μ-messaging layouts with 500 nodes, 4 random sources 🟥 and 78 random targets 🟩 based on different maximum signal range $d_{\max}$. Communication graph $\mathbf{H} = \bigcup_{\forall s \in \boldsymbol{f}(\hat{T})} H_s$ consists of 4 disjoint optimal path trees H_s rooted at different sources 🟥. The arrow ⇠ shows as example a target that is out of signal range (no μ-receiving neighbor in the vicinity). Increasing $d_{\max}$ from 1.1 (left layout, 19 targets not accessible) to 1.25 (right layout) brings about a full coverage for all 78 targets 🟩. In contrast to the μ -layout, the τ-layout is quite confusing arranged due to the overlapping of max. $|\hat{\mathbf{T}}|$=78 communication trees $\{\bar{\mathbf{H}}_t\}_{t \in \hat{\mathbf{T}}}$ resulting to $\bar{\mathbf{H}} = \bigcup_{\forall t \in \hat{T}} \bar{H}_t$.

How about designing a MANET where the paths already traced by the μ-messaging are to use for the τ-messaging? It turns out that this approach is neither advantageous nor efficient:

1. Using μ-paths for τ-messages means
   - storing the nodes' predecessor the μ-message came from and
   - additional search for the τ-message successor (stored as μ-message predecessor) in each node the τ-message arrives

   what increases the total messaging time over a critical limit.



SensRout: 19 sink(s) not reached!! Optimal Sensor Nets with Cost 393.71

SensRout: Optimal Sensor Nets with Cost 362.05

Fig. 4 Distributed Multicast simulation of algorithm **A-SNR:** sources S (🟥) and targets T (🟩). Sensors P \ (S ∪ T) are the white points. If d_{max} is increased from 1.1 to 1.25 then all targets are accessible (lower screenshot).

2. Even for non-mobile nodes it remains dodgy using the μ-paths for the τ-messaging due to a possible failure of nodes ensuring the μ -paths. For this case the nodes have to be equipped with algorithms that react with switching over to the strategy described by **A-SNR** enabling the τ-messaging without using the μ -paths.

6. Conclusion

An advanced path finding algorithm and protocol is given based on a graph theoretical approach. The presented algorithm **A-SNR** intended to be implemented in each node P of a MANET **G** …

- ..neither uses geographic specifications nor assumes that the node nodes are stationary,
- ..globally works as a shortest path algorithm although no path information is stored in an information center or server,
- ..makes available the best forward / backward tracing of queries / answers such that no better path between sources and targets can be found for the actual volatile situation,
- ..eliminates straying messages as soon as possible to prevent a system collapse (due to confined transmission channels each node),
- .. has the least system overhead conceivable and the least negotiation protocol.
- The τ-messaging doesn't rely on the path topology temporarily determined and used during the μ-messaging ⇒ robustness of **A-SNR**!

References

[1] K. Barath-Kuman, J. M. Jaffe: Routing to Multiple Destinations in Computer Networks, IEEE Transactions on Communications, Vol. COM-31, No. 3, March 1983

[2] Sumith Chandratilleke, Michael Kreutzer: "Credential-basierte Ad-hoc- Authentifikation" netzwoche Netzguide E-Security 2003 (März 2003), ISBN 3-907096-04-5

[3] Zouhair El-Bazzal, Michel Kadoch, Basile L. Agba, François Gagnon, Maria Bennani: "An efficient management algorithm for clustering in mobile ad hoc network", International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, Proceedings of the ACM international workshop on Performance monitoring, measurement, and evaluation of heterogeneous wireless and wired networks, Terromolinos, Spain, SESSION: Performance evaluation of wireless networks, Pages: 25-31, Year of Publication: 2006, ISBN:1-59593-502-9, Publisher ACM New York, NY, USA

[4] Leslie D. Fife, Le Gruenwald: "Research issues for data communication in mobile ad-hoc network database systems", ACM SIGMOD Record, Volume 32, Issue 2 (June 2003), Pages: 42 - 47, Year of Publication: 2003, ISSN:0163-5808, Publisher ACM New York

[5] Praveen Gopalakrishnan, Stephanie Demers, Latha Kant: "Speedup techniques for analyzing scalability of large scale mobile ad hoc network management systems" Intern. Conf. On Communications And Mobile Computing, Proceedings of the 2006 intern. conf. on Wireless communications and mobile computing, Vancouver, British Columbia, Canada, SESSION: M2-E: ad hoc-routing, clustering & scalability table of contents, Pages: 299 – 304, ISBN:1-59593-306-9

[6] Tian He, Brian M. Blum, John A. Stankovic, Tarek Abdelzaher: AIDA: Adaptive application-independent data aggregation in wireless sensor networks, ACM Transactions on Embedded Computing Systems (TECS) archive Volume 3 , Issue 2 (May 2004) table of contents. Pages: 426 - 457, Year of Publication: 2004, ISSN:1539-9087

[7] T. He, B. Blum, J. Stankovic, T. Abdelzaher, UoVirginia, USA: AIDA - Adaptive Application Independent Data Aggregation in Wireless Sensor Networks, ACM 2003

[8] W. Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan: Energy-Efficient Communication Protocols for Wireless Microsensor Networks, Proc. Hawaaian Int'l Conf. on Systems Science, January 2000.

[9] W. Heinzelman, Joanna Kulik, and Hari Balakrishnan: Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, Proc. 5th ACM/IEEE Mobicom Conference, Seattle, WA, August 1999.

[10] Chi-Fu Huang, Hung-Wei Lee, Yu-Chee Tseng: "A two-tier heterogeneous mobile Ad Hoc network architecture and its load-balance routing problem" Mobile Networks and Applications, Volume 9, Issue 4 (August 2004), Pages: 379 - 391 ISSN:1383-469X, Publisher: Kluwer Academic Publishers Hingham, MA, USA

[11] Ch. Intanagonwiwat, R. Govindan, D. Estrin, USC, Califomia: Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks, ACM 2000

[12] M. Kähmer, S.Höhn, M.Kreutzer, ALU Freiburg, Germany: Sicherheit in UbiComp -Sicherheits-Framework (German-spoken), 08/2004

[13] Chris Kar1and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berke1ey, USA. May 2003

[14] M. Kreutzer, M. Kähmer, ALU Freiburg, Germany: Ubiquitous Computing Techno1ogy in an Infrastructureless Environment, 2004

[15] Kyu-Hwan Lee, Jae-Hyun Kim, jun-Hee Park, Dong-Hee Kim, Kyung Duk Moon: "Routing based authentication for mobile ad hoc network in home environment", Conference on ubiquitous information management and communication, Proceedings, Suwon, Korea, SESSION: Security, Pages 334-338, Year of Publication: 2008, ISBN:978-1-59593-993-7, published by ACM

[16] Prasanna Padmanabhan, Le Gruenwald, Anita Vallur, Mohammed Atiquzzaman : "A survey of data replication techniques for mobile ad hoc network databases" The VLDB Journal — The International Journal on Very Large Data Bases archive Volume 17, Issue 5 (August 2008) Pages: 1143 - 1164 ISSN:1066-8888 Springer-Verlag New York, Inc.

[17] Amir Spahic, Michael Kreutzer, Martin Kiähmer, Sumith Chandratilleke: "Pre-Authentication Using Infrared" Pervasive 2004, SPPC: Workshop on Security and Privacy in Pervasive Computing, Vienna to be published by Kluwer

[18] Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen, Jang-Ping Sheu: "The broadcast storm problem in a mobile ad hoc network", Wireless Networks, Volume 8, Issue 2/3 (March-May 2002), Selected Papers from Mobicom'99, Pages: 153 - 167, ISSN:1022-0038

[19] Qunwei Zheng, Xiaoyan Hong, Sibabrata Ray: "Recent advances in mobility modeling for mobile ad hoc network research", ACM Southeast Regional Conference, Proceedings of the 42nd annual Southeast regional conference, Huntsville, Alabama, Session: Special session on mobile computing #3, Pages: 70-75, Year of Publication: 2004, ISBN:1-58113-870-9, Publisher ACM New York