Detecting Selfish and Malicious Nodes in MANETs

Martin Schütte

***Abstract*— Mobile ad-hoc networks (MANETs) rely on cooperation of all participating nodes. Thus they are vulnerable to selfish nodes using the net without providing own ressources, as well as malicious nodes attacking the net infrastructure.**

This paper outlines important attacks and summarizes popular approaches to design secure MANET protocols in order to detect selfish and malicious nodes and to enforce cooperation.

I. Introduction: Used Terms and Definitions

A. Nets

A mobile ad-hoc network (MANET) is a wireless network among mobile devices. In designing a MANET the following requirements should be met as far as possible [1] [2, p. 13ff]:

- all nodes are regarded as equal, forming a peer-to-peer net without dedicated servers or routers,
- all nodes are mobile, thus the net's topology is changing over time,
- the net is too big for direct communication between every pair of nodes, thus multi-hop communication is required,
- the net is dynamic (nodes may join or leave the net at any time) and self-organizing,
- the net is publicly accessible, thus
- participating nodes may not have to be pre-authorized and unknown clients may be allowed to join the net,
- nodes may consist of a wide range of devices with different ressources (including PCs, laptops, PDAs, cellphones)

In addition I will sometimes refer to hybrid MANETs, meaning a MANET with one or more fixed basestations which might provide additional services or act as a gateway into other nets (cf. section V).

B. Nodes

As there is no dedicated infrastructure or central coordination, the nodes have to cooperate and self-organize to form a working communication network. Communication only works if nodes participate and forward other node's packets. On the other hand every node has to consider its limited ressources (most notably its energy). So every node is motivated to contribute as litte as possible of its own energy.

Usually, it is expected that all nodes forward as needed, but other policies are possible as well (e. g. only require forwarding as long as a node's battery level is high). In any way the MANET's protocols and policies imply a normative expectation on every participating node a) to behave according to agreed protocols and b) to forward a fair amount of other node's packets as needed.

As long as all nodes adhere to this and cooperate, the MANET should work without problems. One of the most important issues in designing MANET protocols is how to deal with nodes that do not cooperate. Depending on their (or their user's) motivation I will categorize these nodes into three groups:

- Malevolent nodes – Nodes that want to compromise the security of the MANET or of other nodes. Their actions are directed on some desired effect, but they are generally not rational because they do not strive for their own benefit maximization.
- Selfish nodes – Nodes that do not forward other's packets, thus maximizing their benefit at the expense of all others. They are assumed to always behave rationally, so they cheat only if it gives them an advantage.
- Erroneous nodes – These are nodes with failing hardware or incorrect software. They do not intentionally misbehave but if they impair the working of the net, then they have to be treated just as malevolent or selfish nodes.

C. Cryptography and Security

Most techniques presented here need cryptographic algorithms in order to be securely and reliably implemented. A basic understanding of symmetric and asymmetric (or public-key) encryption, key chains, message authentication, digital

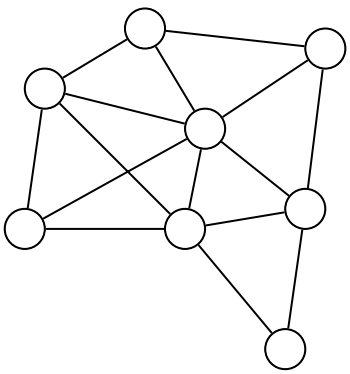

Fig. 1. A highly connected net

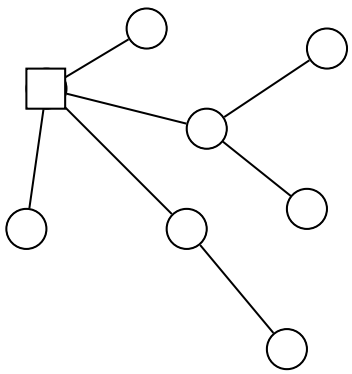

Fig. 2. A hybrid net degraded ino a tree

signatures, and threshold cryptography are useful to appreciate the possibillities and consequences of these methods. (Introductory remarks on these topics can be found in [3]–[5].)

In order to define attacks a traditional understanding of host and network security is presumed as well. A system is considered secure if it ensures confidentiality, integrity, availability, and accontability of all actions. Any action that assaults this security is considered an attack [4], [5].

D. Rational Choice

In order to understand a node's motivation and to analyze different protocols a common approach is to use concepts from rational choice theory and game theory. These theories suppose that all events can be associated with a benefit and all participants know about all possible consequences of their actions; thus all participants can rationally chose a behaviour (or strategy) that maximizes their own benefit.

A well known scenario from game theory is the prisoner's dilemma where two persons (or players) have to decide wether to cooperate or betray each other. If they cooperate then they will both benefit, if only one of them defects then the traitor will get an even higher benefit while the loyal one looses, if both betray then there is no benefit for either one. By rational choice both players have to betray each other thus missing the possible benefit. They arrive at this choice, because it is the only Nash equilibrium – the point where no single player can increase his benefit by changing his strategy.

The analogy to a simple MANET with two nodes should be obvious: the nodes can either cooperate thus getting the benefit of a working net, one can betray by not forwarding the other's packets thus one is getting the bigger benefit of communicating without commiting own ressources (free-riding) and the other one looses, or they can both refuse to cooperate and no net is formed.

So the basic challenge of MANET protocols is to change the rules in such a way to create a Nash equilibrium with nodes cooperating [6], [7]. In social communities there are two ways to attain conformance: either by rewarding desired actions and behaviour or by sanctioning deviant actions and behaviour. As both rewards and sanctions come at some cost they usually should be avoided; thus the first alternative is preferable if conformance is not to be expected and rewards are not too costly, the latter alternative is preferable if conformance is already the norm and deviations are the exception [9, p. 90ff.]. Likewise there are two approaches for creating MANET protocols: either assume cooperation and detect selfish nodes (resulting in reputation systems and intrusion detection) or assume non-cooperation and create an incentive to cooperate (resulting in trading systems).

II. Attacks

I will now categorize and describe possible attacks on MANETs. Most descriptions are intentionally abstract as I do not want to analyze specific protocols but list general attacks on all kinds of MANETs and protocols.

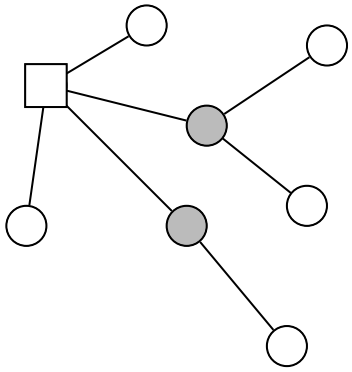

Fig. 3. A hybrid MANET with routes to/from the gateway: very few nodes (grey) actually have to forward other nodes' data.

A. Passive Attacks

1) Eavesdropping: The simplest attack on a wireless net is eavesdropping; it requires minimal preparation and cannot be detected.

Eavesdropping can be subdivided as follows:

1) The content of communication. As there exist various techniques to encrypt the content, guaranteeing its confidentiality is not difficult. As encryption is an expensive operation users of mobile clients might choose not to encrypt in order to save computing and energy ressources.
2) Infrastructure meta-data, including used protocol options and especially routing information. Encrypting this communication is possible, but usually not worth it because it would require sophisticated key management among the participants.
3) Amount and distribution of communication or location of node. Even without knowing any content, an eavesdropper can still detect traffic patterns among the nodes. In theory this could be avoided by randomly sending messages between nodes but in mobile environments this is infeasable due to energy constraints. Depending on the MANET's use and policy even the disclosure of a node's location might be considered a successful security breach.

2) Non-Participation: After joining the MANET a node could simply refuse to forward other node's data (often called *free riding*, [11]). There are two alternatives:

1) The node does not respond to route request messages. – This is a selfish behaviour but it does not impair the net as it will find another (maybe suboptimal) route.
2) The node does respond to route request messages, but when becoming part of a route it silently discards the data it is supposed to forward. – This works well because all nodes are supposed to forward data, but most nodes are at the perimeter and only few nodes are actually part of used routes inside the net (cf. Fig. 3).

Simulations show that existing (non-secure) MANET protocols are very vulnerable to the second strategy, as it reduces the net's throughput significantly [8, p. 20ff] [3, p. 88ff].

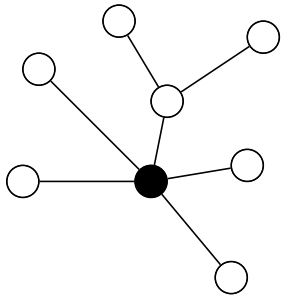

Fig. 4. *Black hole* attack

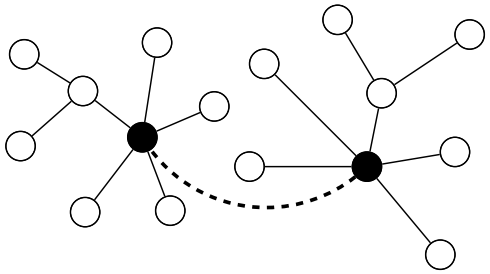

Fig. 5. *Wormhole*

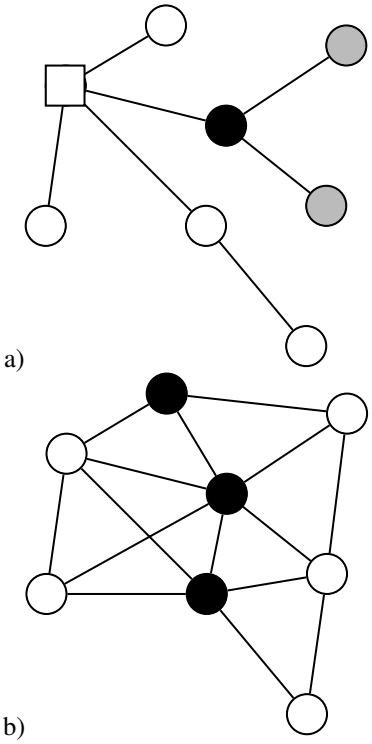

Fig. 6. *Eclipse* attack: a) one malicious node (black) controlling two others (grey), b) three malicious nodes (black) bipartitioning the net

B. Active Attacks

- Denial of Service. With enough ressources an attacker can always send more data than other nodes can process. Mobile clients are especially vulnerable to denial of service attacks because it quickly drains their energy reserve. Another possible approach does not even need to send large amounts of data but just sending enough packets to prevent a node from going into sleep- oder energy saving-mode; this is called *sleep deprivation*.
- Manipulate forwarded data. This is an potentially dangerous attack but quite simple to prevent by using message authentication.
- Manipulate routing meta-data.
  - *Simple denial of service* – some routing protocols allow very simple attacks, like sending data for non-existing targets, thus creating a route-finding broadcast.
  - *Black hole* – a node can announce itself as having the shortest path to all other nodes, thus it disrupts existing routes and attracts much traffic. Getting a large amout of data leads to new opportunities like selectively forwarding/dropping packets (sometimes called *grey hole*) or various kinds of traffic and content analysis [12].
  - *Wormhole* – collaborating attackers can create two or more black holes and connect them (out of band, e. g. by directional antennae or wire). This gives them control over large parts of the MANET and its packets [13], [14].
  - *Eclipse* – collaborating attackers can partition the net, thus controlling all data flowing between the partitions. Depending on the number of attackers one can seperate single nodes, get between a basestation and its clients or even bipartition a large net [15].
- *Sybil* attack – a single malicious node can simulate a number of independent nodes. This is basis for a lot of manipulations: it favours the client in bandwith allocation, gives influence on routing decisions, and undermines every kind of voting algorithm or threshold cryptography [16]–[18].

III. Detection and Prevention

A. Watchdog

With this simple approch a node sends a packet to its neighbour and then overhears the neighbour forwarding it one hop further along the route. Thus a misbehaving node dropping or manipulating packets is immediately identified and routes using this node can be avoided (using a so-called pathrater component to chose the best route) [19].

Unfortunately this mechanism is too simple and has two major drawbacks. First: it is error-prone; a packet collision between AB causes a false negative detection (A does not recognize successful retransmission) and a collision between BC causes a false positive detection (A acknowleges the retransmission even though it failed). The model also relies on all clients to have equal sending ranges – this conflicts with modern WiFi-controllers using energy control. Second: When a node recognizes its neighbour as non-participating it does not spead this information, but is only supposed to find a new route arround the problem, thus even rewarding the non-participating node (now it does not have to forward other node's data anymore). For the node on its own it is perfectly rational to avoid the selfish node and increase its own throughput – but for the net at large this is a bad choice

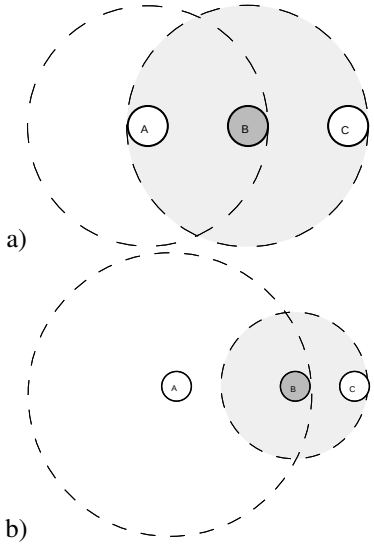

Fig. 7. Watchdog (the shaded area is B's radio range): a) with equal ranges A can overhear B's retransmission; b) with power control A cannot overhear B's retransmission

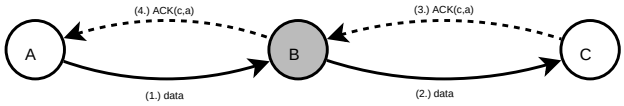

Fig. 8. 1. A sends for C; 2. B has to forward the packet as it does not know if it contains an acknowledgement request; 3. C confirms the retrieval with its private key; 4. B forwards the acknowledgment back to A

as it does not punish the selfish node but only burdens the cooperating ones with more work.

B. Random Feedback

If one assumes a working key management among all nodes, then nodes can acknowledge forwarded packets across multiple hops.

Say nodes A, B and C are part of a route. Now A can include an encrypted nonce for C in every packet and C can acknowledge each received packet with the correct nonce. B as the intermediate node cannot decrypt the nonce, thus it either has to correctly forward the packet (and C's acknowledgement) or is immediately recognized as a cheater.

Since verifying every packet this way is too expensive, the scheme can easily be refined with A selectively requesting the acknowledgement. If this request is encrypted as well, then B has to forward all packets because it can not determine which ones include a request. A suitable algorithm could begin with frequent checks to see if a node is dependable and later use longer, random intervals between checks. [20]

C. Distributed Reputation

The weakness of Watchdog led to distributed algorithms with every node periodically collecting ratings about its neighbours, distributing its ratings and then calculating reputation values from its own and other nodes' ratings.

Every step can be done in many different ways and there exist many different protocols to determine a distributed reputation. The most important ones are **Co**llaborative **Re**putation

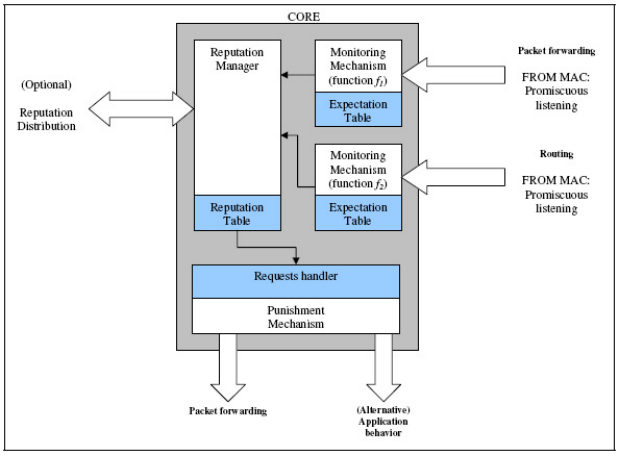

Fig. 9. CORE architecture [8, p. 71]

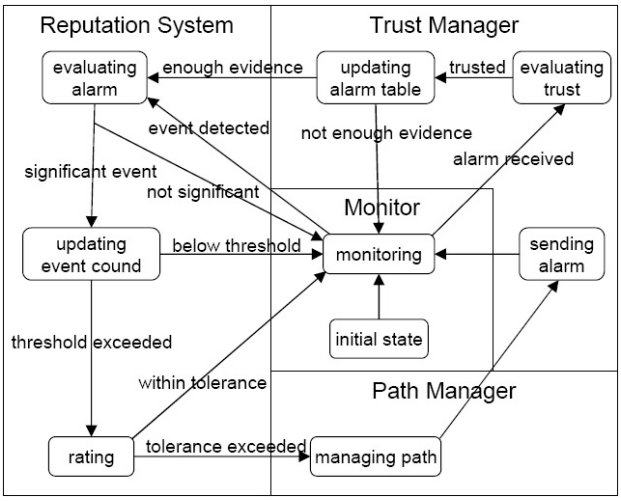

Fig. 10. CONFIDANT architecture [2, p. 92]

Mechanism (CORE, [8]) and **C**ooperation **O**f **N**odes – **F**airness **I**n **D**ynamic **A**d-hoc **Net**works (CONFIDANT, [2]).

Both consist of four modules, slightly differently named in CORE and CONFIDANT (cf. Fig. 9,10):

- Monitoring: collect first-hand information about neighbours, unfortunately this step usually relies on Watchdog,
- Reputation Manager or Reputation System: process monitoring data and update a reputation table,
- Reputation Distribution or Trust Manager: exchange reputation values with other nodes,
- Requests Handler or Path Manager: decide which path to chose and which packets to forward.

The used algorithms are well studied and simulations show them to be mature and usable protocols – although it should be noted that they only exist on paper and as GloMoSim-modules. As both protocols are under some criticism (mostly for their use of Watchdog and their underlying assumptions) there still needs to be an actual implementation to show their fitness in real MANETs. (An implementation of CONFIDANT was planned but not yet published; an experimental testbed implementation of CORE was recently presented [21].)

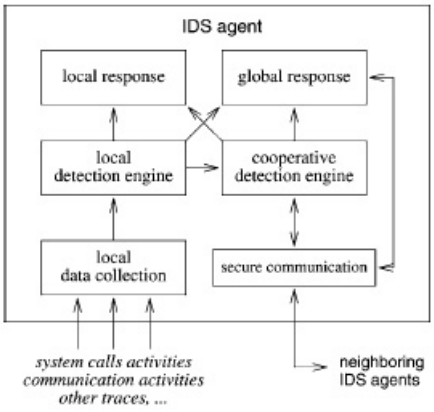

Fig. 11. A conceptual model for an IDS agent [22]

D. Mobile IDS

If one were given all events in a MANET like nodes joining/leaving, route requests/replies, amount of errors, packets and data etc. then an observable pattern of normal net operation as well as other observable patterns for various anormalities and attacks might be assumed.

It is suggested that every node runs an intrusion detection agent that collects network events, analyses them, shares its data with other nodes' agents, and derives appropriate responses to detected attacks (cf. Fig. 11). First the system has to be trained with data from normal network operation. From then on the collected data is analyzed by calculating the information-theoretic entropy and conditional entropy. If the conditional entropy from recent measurements differ from the previously trained values then an abnormality is detected and a reaction can be initiated.

Once a local abnormality is detected it should be passed to neighbouring nodes. By exchanging their data the mobile IDS agents should be able to detect abnormalities more accurately and to initiate not only local but a global reaction (e. g. excluding a malicious node from the MANET). [22]

E. Currency Systems

While most techniques try to identify and punish misbehaviour, there are also approaches to provide an incentive for good behaviour (cf. Section I-D). These schemes use some kind of currency to reward cooperation and contributions (forwarding data) and on the other hand they require payment for generated traffic (sending or receiving data).

Three proposed protocols using a currency system shall be mentioned here: NUGLETS [23] is probably the first protocol of this kind; the protocol itself and the questions raised by its authors are basic to all other currency systems. The most notable concept is that of a tamper-proof hardware module, which schould be included in all devices to ensure proper payment and to prevent fraud – thus there is no need for a central clearinghouse and the protocol is completely decentralized. The second system is SPRITE (a **s**imple cheat-**p**roof c**r**edi**t**-based syst**e**m) [24] which does not need the tamper-proof hardware, but proposes a central Credit Clearance Service to track all network messages and handle the accounting. At last there is a hybrid scheme CASHNET (**C**ooperation and **A**ccounting **S**trategy for **H**ybrid **Net**works) [25] requiring both tamper-proof hardware (in form of a smartcard) as well as central servers; yet this is one of the few protocols actually implemented [26].

The two main targets for these systems are security (it must not be possible to cheat the system) and incentive (all payments have to be balanced to motivate the nodes to cooperate).

While the security can usually be ensured by cryptography, the optimal incentive is somewhat harder to achieve as it depends on many factors. The topology of the net itself can make a big difference: In highly connected nets where all nodes send and receive roughly the same amount of data, a simple payment by volume works well. In degraded nets a balanced algorithm for payment has to be much more complex. If a MANET spreads around a gateway, then the inner nodes automatically get the chance to forward others' data while the outer nodes do not get this chance but still have to pay for their own communication (cf. Fig. 2).

IV. PROBLEMS

While the previous chapters dealt with problems of technical nature for which technical sulutions might be envisaged, I now want to present a set of more difficult problems regarding the policies of MANETs. These problems can be reduced to mutually exclusive requirements; thus the participants have to decide which requirement gets higher priority because all solutions are necessarily trade-offs.

A. Identity

Just like social relations a nodes reputation in a MANET is tied to a fixed identity and recognizability. Thus any property used as an identifier for an object or device has to meet strict requirements: it usually has to be unique, long living and impossible to change or transfer onto another object [3, p. 117].

It is easy to see that such identifiers cannot be created by the device itself but have to be assigned by a trusted third party. In practice this third party is implemented by a central certification authority (CA) which verifies identities and associated keys.

This holds at least for all nets in which nodes are generally trusted and only detected perpetrators are punished; in that case an easy change of identity would render every punishment useless. One might argue that fixed identities are not as important in nets based on currency systems. In these nets a node does not benefit from changing its identity but rather loses its previously earned status.

Now although implementing a CA can be seen as a purely technical task, it leads to even further questions, most notably how to preserve the users' privacy. Having a unique identification in large MANET makes it easy to track a specific user, including his movement and data exchange. The easiest way to prevent this is using pseudonym identities that a node can use instead of its 'real' one, but as these also have to be signed by the CA the administartive overhead gets even bigger [3,

ch. 9]. The dilemma of identity vs. privacy is one of the most fundamental questions in every network design and probably will not be resolved in the near future.

A very important developement is the Trusted Computing Group (TCG, formerly Trusted Computing Platform Alliance/TCPA) initiative to embedd so called Trusted Platform Modules into computers and mobile devices [28]. These modules basically provide a unique public/private key-pair signed by the TCG as well as means to use sub-keys as pseudonyms to enhance privacy.

B. Location

Another requirement may be the (im)possibility to determine the location of a node either topologically in the MANET or geographically on campus/inside the building.

Information about the net topology is useful for all clients. Participating nodes will find it easier to find optimal routes or to detect attackers if they can 'see' a large part of the net; on the other hand an intruder can use the same information to find promising approaches for its attack such as basestations, important routing nodes, or especially weakly connected parts of a net.

Geographical information can be determined by cooperating nodes or basestations. With directed antennae it is quite easy to localize a nearby target nde by taking a cross bearing. With omnidirectional antennae localization is more difficult but can be achieved by comparing the target's signal strengths at many known nodes or basestations [3, p. 136 ff.] [29, for 801.11 nets]. There are several reasons to collect geographical information, e. g. to detect Sybil attacks, to check wether a routing algorithm finds the geographically optimal routes, or just to measure the spatial extension of the MANET. On the other hand this information can be used to track a device's movements, impairing the privacy of its user. By tracking the positions of PDAs in a company MANET it would be easy to see who sits in the cafeteria instead of the office or who leaves early from work.

C. Different Ressources

One advantage of MANETs is their ability to connect very different kinds of devices. Desktop PCs, Laptops, or PDAs – everything with a wireless network interface (like IEEE 802.11 or Bluetooth) and the necessary overlay drivers for the used MANET protocols can access the same MANET and communicate with each other. As long as all nodes cooperate it is desirable to use their different ressources for common benefit, e. g. letting more powerful laptops route traffic for smaller PDAs.

Unfortunately it usually has to be assumed that some nodes are malicious and do not cooperate – then it becomes dangerous to have more powerful devices. Now the very same scenario of one laptop routing for many PDAs gives that laptop a good position to launch an attack (either against the PDAs or against the MANET at large).

V. Hybrid MANETs

At last I want to give some advantages of a hybrid MANET, i. e. a MANET with one or more fixed basestations.

- Basestations can act as gateways into wired nets, usually providing access to the Internet. This also makes them the most suitable places for traditional intrusion detection systems.
- Multiple basestations can be connected by directed antennae or wired net, thus forming a backbone and enlarging the range of the MANET.
- Basestations can simplify the routing, e. g. by keeping track of all participating nodes.
- Basestations can act as a CA, keyserver, clearinghouse, or other trusted instance for distributed processes.

As a secondary effect MANETs with gateways often have different traffic patterns. Instead of the archetypical MANET with every node communication at random with all other nodes, a MANET with gateway can have a very simple communication structure with all nodes only talking to the gateway. In this case the fully connected net degraded into a spanning tree with the gateway as its root. If this is expected, then the routing becomes substantially simpler – every packet can be forwarded up to the root and then down to the receiving node.

On the other hand fixed basestations raise the problem of *Single Points of Failures* – all advantages are lost if a MANET has to rely on a single basestation. Thus a hybrid MANET should always have several redundant basestations and if the net is important then the basestations themselves should use only redundand ressources (i. e. if they act as gateways they should have two different Internet uplinks using different switches, if they act as a clearinghouse they should use a highly available database).

VI. Conclusion

Many explicit or implicit requirements on MANETs are mutually exclusive. Implementing such a net always requires decisions and trade-offs. Probably the most important decision is wether to require fixed identities, since a number of protocols rely on this for accountability and recognizability of participants and their actions.

The very basic properties of wireless communication and the necessary self-organization of MANETs lead to some weaknesses that can be abused for attacks. Even with mature and security-aware protocols it is very hard to mitigate this kind of attacks as the trade-offs might be too big (always considering the limited ressources of mobile devices). Besides security considerations it is just as essential to create incentives for node cooperation, as the net has to rely on it.

Many protocols were suggested to enforce cooperation and as to detect misbehaving nodes. All of them make certain premises which makes them more suitable for some scenarios and less suitable for others. As only few of them are actually implemented their evaluation is mostly based on simulations and there is no first-hand experience on their effect on real and sufficently large MANETs.

When implementing a MANET the issue of basestations and central services is another major issue as it usually determines the choice of protocols. Fixed basestations can be gateways to access other nets and many services that are hard to implement by distributed algorithms can be moved to central servers; this comes at the cost of reduced redundancy and bigger dependence on the availability of single access points.

REFERENCES

[1] J.-P. Hubaux, T. Gross, J.-Y. L. Boudec, and M. Vetterli, "Toward self-organized mobile ad hoc networks – the terminodes project," *IEEE Communications Magazine*, vol. 39, no. 1, pp. 118–124, 2000.

[2] S. Buchegger, "Coping with misbehavior in mobile ad-hoc networks," Ph. D. Thesis, EPF Lausanne, Apr. 2004. [Online]. Available: http://www.sims.berkeley.edu/~sonja/phdThesis.pdf

[3] F. Kargl, "Sicherheit in Mobilen Ad-hoc Netzwerken," Doktorarbeit, Universität Ulm, 2003. [Online]. Available: http://vts.uni-ulm.de/doc.asp?id=3704

[4] W. Stallings, *Network and Internetwork Security*. New Jersey: Prentice-Hall, 1995.

[5] C. Eckert, *IT-Sicherheit*. München: Oldenbourgh, 2001.

[6] J. Leino, "Applications of game theory in ad hoc networks," Diplomarbeit, Helsinki University of Technology, 2003. [Online]. Available: http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/988/

[7] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Experiences applying game theory to system design," in *PINS '04: Proceedings of the ACM SIGCOMM workshop on Practice and theory of incentives in networked systems*. New York, NY, USA: ACM Press, 2004, pp. 183–190. [Online]. Available: http://doi.acm.org/10.1145/1016527.1016531

[8] P. Michiardi, "Cooperation enforcement and network security mechanisms for mobile ad hoc networks," Thesis, Ecole Doctorale d'Informatique, Télécommunications et Électronique de Paris, Dec. 2004. [Online]. Available: http://pastel.paristech.org/archive/00001114/

[9] H. Popitz, *Phänomene der Macht*. Tübingen: Mohr Siebeck, 1992.

[10] A. Urpi, M. Bonuccelli, and S. Giordano, "Modelling cooperation in mobile ad hoc networks: a formal description of selfishness," in *WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003, INRIA Sophia-Antipolis, France*, 2003.

[11] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, "Free-riding and whitewashing in peer-to-peer systems," in *PINS '04: Proceedings of the ACM SIGCOMM workshop on Practice and theory of incentives in networked systems*. New York, NY, USA: ACM Press, 2004, pp. 228–236. [Online]. Available: http://doi.acm.org/10.1145/1016527.1016539

[12] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks," in *ACM-SE 42: Proceedings of the 42nd annual Southeast regional conference*. New York, NY, USA: ACM Press, 2004, pp. 96–97. [Online]. Available: http://doi.acm.org/10.1145/986537.986560

[13] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security*. New York, NY, USA: ACM Press, 2004, pp. 51–60. [Online]. Available: http://doi.acm.org/10.1145/1023646.1023657

[14] I. Khalil, "Liteworp: A lightweight countermeasure for the wormhole attack in multihop wireless networks," in *DSN '05: Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05)*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 612–621. [Online]. Available: http://dx.doi.org/10.1109/DSN.2005.58

[15] A. Singh, M. Castro, P. Druschel, and A. Rowstron, "Defending against eclipse attacks on overlay networks," in *EW11: Proceedings of the 11th workshop on ACM SIGOPS European workshop: beyond the PC*. New York, NY, USA: ACM Press, 2004, p. 21. [Online]. Available: http://doi.acm.org/10.1145/1133572.1133613

[16] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems: First International Workshop, LNCS 2429*, A. R. P. Druschel, F. Kaashoek, Ed. Springer-Verlag, Jan. 2002, pp. 251–260. [Online]. Available: http://www.springerlink.com/openurl.asp?genre=article&issn=0302-9743&volume=2429&spage=251

[17] B. Prêtre, "Attacks on peer-to-peer networks," 2005. [Online]. Available: http://dcg.ethz.ch/theses/ss05/freenet.pdf

[18] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *IPSN '04: Proceedings of the third international symposium on Information processing in sensor networks*. New York, NY, USA: ACM Press, 2004, pp. 259–268. [Online]. Available: http://doi.acm.org/10.1145/984622.984660

[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM Press, 2000, pp. 255–265. [Online]. Available: http://doi.acm.org/10.1145/345910.345955

[20] D. Djenouri, N. Ouali, A. Mahmoudi, and N. Badache, "Random feedbacks for selfish nodes detection in mobile ad hoc networks, LNCS 3751," in *Operations and Management in IP-Based Networks: 5th IEEE International Workshop on IP Operations and Management, IPOM*. Springer-Verlag, 2005, pp. 68–75. [Online]. Available: http://dx.doi.org/10.1007/11567486_8

[21] C. Lavecchia, P. Michiardi, and R. Molva, "Real life experience of Cooperation Enforcement Based on Reputation (CORE) for MANETs," in *IEEE REALMAN 2005, IEEE ICPS Workshop on Multi-hop Ad hoc Networks: from theory to reality in conjunction with IEEE ICPS 2005, July 14, 2005, Santorini, Greece*, July 2005. [Online]. Available: http://www.cl.cam.ac.uk/Research/SRG/netos/realman/05/docs/REALMAN05_proceedings.pdf

[22] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks," *Wirel. Netw.*, vol. 9, no. 5, pp. 545–556, 2003. [Online]. Available: http://dx.doi.org/10.1023/A:1024600519144

[23] L. Buttyán and J.-P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Jan. 2001. [Online]. Available: http://icwww.epfl.ch/publications/documents/IC_TECH_REPORT_200101.pdf

[24] Y. R. Y. Sheng Zhong, Jiang Chen, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," 2003. [Online]. Available: http://www.cse.buffalo.edu/~szhong/papers/sprite.pdf

[25] A. Weyland, "Cooperation and accounting in multi-hop cellular networks," Inauguraldissertation, Universität Bern, 2006. [Online]. Available: http://www.iam.unibe.ch/~rvs/research/pub_files/We05.pdf

[26] C. Latze, "Linux implementation of a cooperation and accounting strategy for multihop cellular networks," Diplomarbeit, Universität Bern, 2006. [Online]. Available: http://www.iam.unibe.ch/~rvs/research/pub_files/La06.pdf

[27] W.-C. Liao, F. Papadopoulos, and K. Psounis, "An efficient algorithm for resource sharing in peer-to-peer networks." in *Networking*, ser. Lecture Notes in Computer Science, F. Boavida, T. Plagemann, B. Stiller, C. Westphal, and E. Monteiro, Eds., vol. 3976. Springer, 2006, pp. 592–605. [Online]. Available: http://dx.doi.org/10.1007/11753810_50

[28] Trusted Computing Group, "Trusted Platform Module (TPM) Specifications," 2003. [Online]. Available: https://www.trustedcomputinggroup.org/specs/TPM

[29] A. Haeberlen, E. Flannery, A. M. Ladd, A. Rudys, D. S. Wallach, and L. E. Kavraki, "Practical robust localization over large-scale 802.11 wireless networks," in *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM Press, 2004, pp. 70–84. [Online]. Available: http://doi.acm.org/10.1145/1023720.1023728

[30] G. F. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: a survey," *Wireless Communications and Mobile Computing*, vol. 6, no. 3, pp. 319–332, 2006.