

Intrusion tolerance in Publish/Subscribe based MANET

Erland Kolstad

Agenda

- Why study publish/subscribe based MANET?
- Introduction to publish/subscribe networks
- Possible attacks on the protocol
- Presentation of findings
- Protocol enhancements
- Conclusion
- Questions

- **Why study publish/subscribe based MANET?**
- Introduction to publish/subscribe networks
- Possible attacks on the protocol
- Presentation of findings
- Protocol enhancements
- Conclusion
- Questions

Why publish/subscribe based MANET?

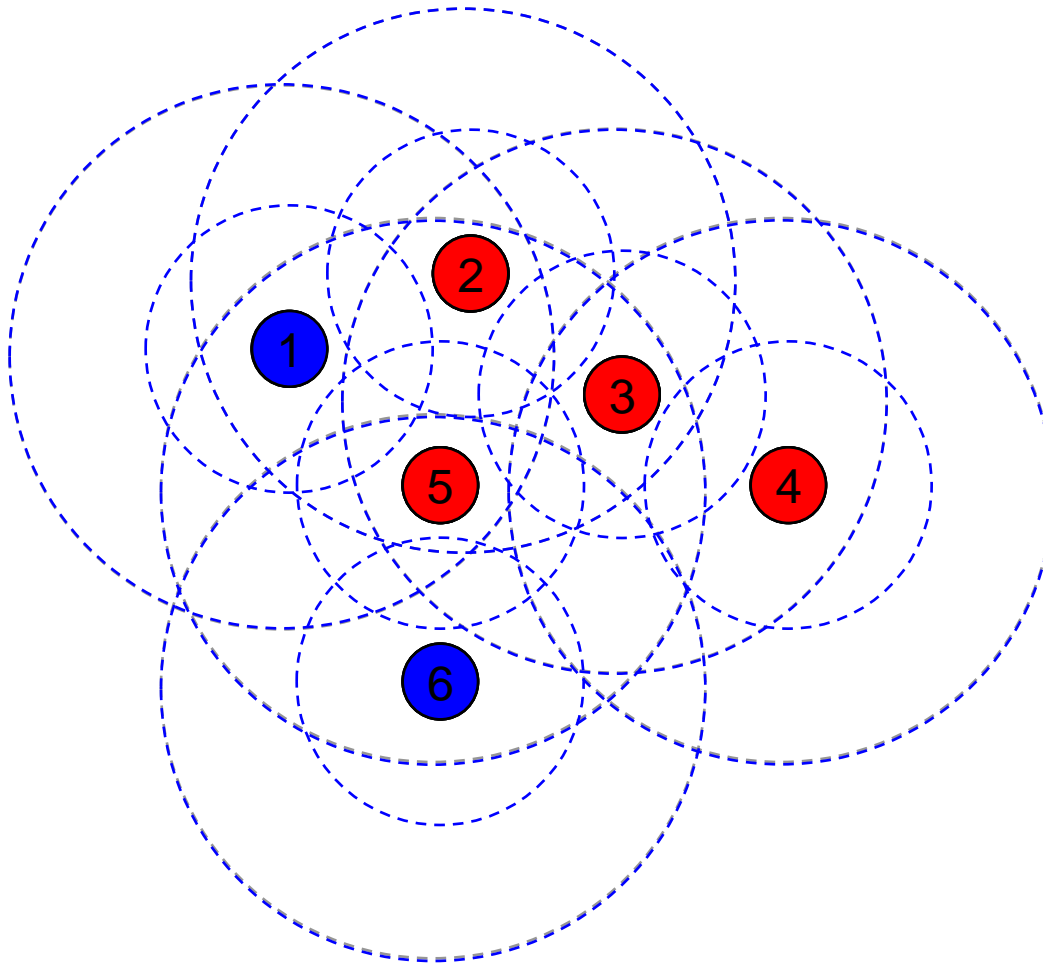
- Accurate information and efficient distribution of relevant information is of the utmost importance in many operations to achieve information supremacy
- Many operations require rapid network establishment and frequently network topology changes
- In mobile networks it is important to keep routing overhead at a minimum
- Mobile networks require filtering mechanisms and efficient message distribution to keep network load at a minimum
- Publish/subscribe networks have good qualities to support those goals

- Why study publish/subscribe based MANET?
- **Introduction to publish/subscribe networks**
- Possible attacks on the protocol
- Presentation of findings
- Protocol enhancements
- Conclusion
- Questions

Previous work

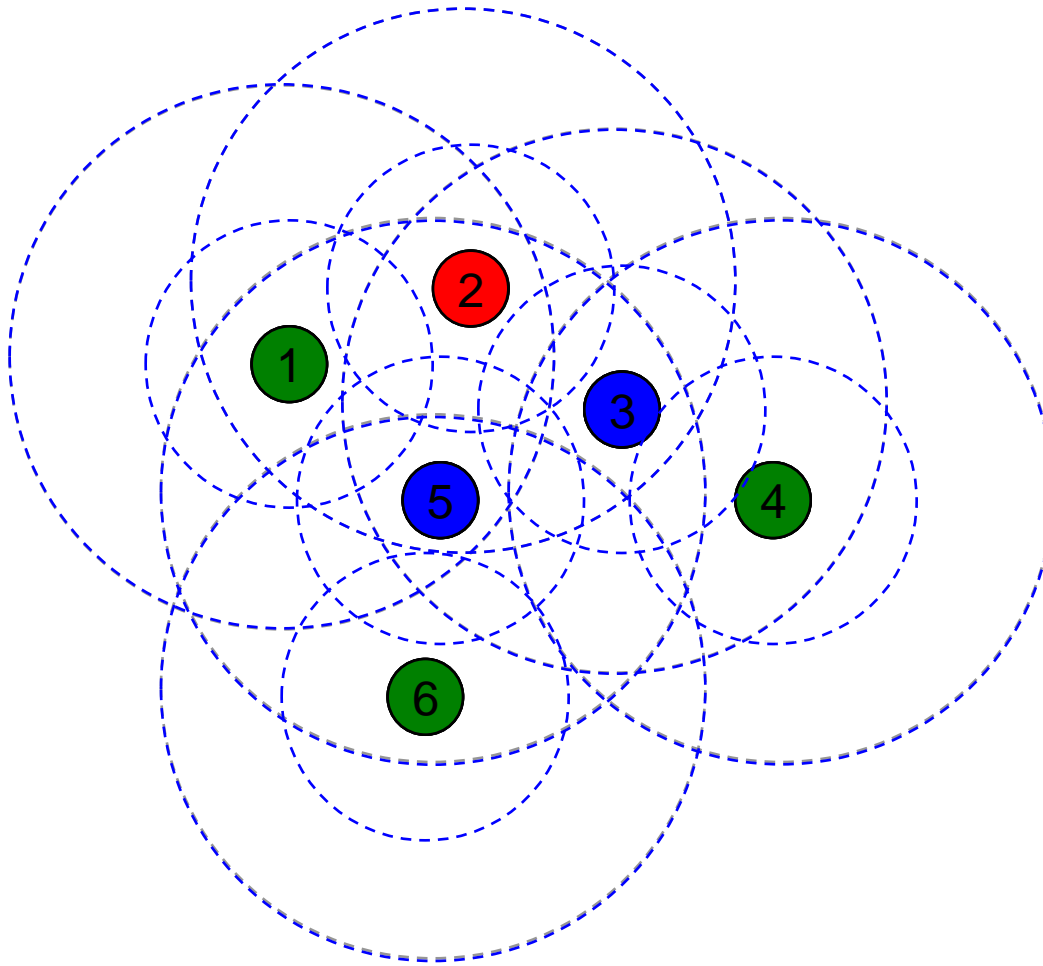
- Very little work done on intrusion tolerance in publish/subscribe networks
- Previous work primary focus on failures and not on attacks
- Previous analyzed protocols are not suited for message distribution in networks with many publishers, which publish within same information theme
 - They require building multicast trees for each publisher
- Protocol proposed by Fongen is designed to also work in such scenarios

Message subscription



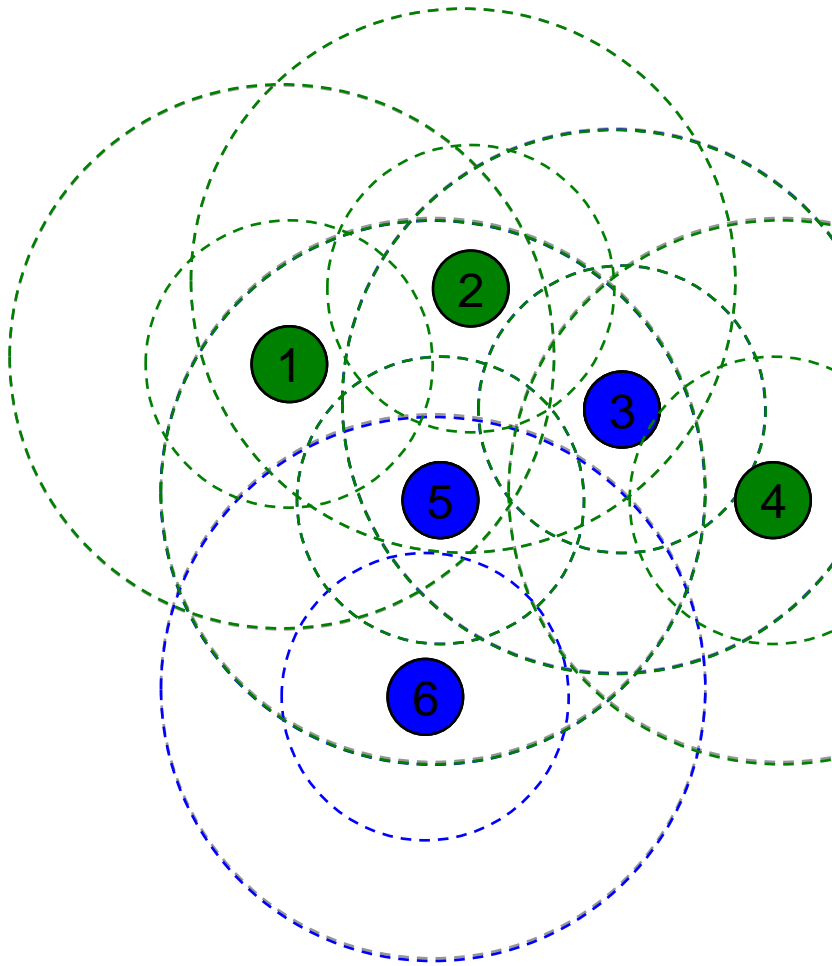
Node	Theme	ID	Source
1	A	123	2
	A	123	5
2	A	123	3
3	A	123	4
4	A	123	OWN
5	A	123	3
6	A	123	5

Message subscription



Node	Theme	ID	Source
1	A	123	2
	A	123	5
	A	234	2
2	A	123	3
	A	234	OWN
3	A	123	4
	A	234	2
4	A	123	OWN
	A	234	3
5	A	123	3
	A	234	2
6	A	123	5
	A	234	5

Message distribution



MsgID	#ACK	Node	Theme	ID	Source
A-333	0	1	A	123	2
			A	123	5
			A	234	2
A-333	0	2	A	123	3
			A	234	OWN
A-333	0	3	A	123	4
			A	234	2
A-333	0	4	A	123	OWN
			A	234	3
A-333	0	5	A	123	3
			A	234	2
A-333	0	6	A	123	5
			A	234	5

- Why study publish/subscribe based MANET?
- Introduction to publish/subscribe networks
- **Possible attacks on the protocol**
- Presentation of findings
- Protocol enhancements
- Conclusion
- Questions

Possible attacks

- Jamming
- Stop forwarding messages
- Stop forwarding DATA-messages
- False ACK-messages
 - Random
 - False ACK based on network knowledge
 - Sending many ACK to manipulate ACK count
- Introduce false DATA-messages
- Wiretapping
- Overloading the network

- Why study publish/subscribe based MANET?
- Introduction to publish/subscribe networks
- Possible attacks on the protocol
- **Presentation of findings**
- Protocol enhancements
- Conclusion
- Questions

Experiment

- Protocol implemented in the NS-2 network simulator
- Node location within simulation grid and message subscription/generation was created randomly
- Attacker was chosen randomly among nodes in the network

Baseline

<i>Area size</i>	<i>Number of nodes</i>	<i>Number of silent nodes</i>	<i>Baseline delivery rate</i>	<i>Delivery rate with radio silent nodes</i>	<i>Delivery rate change</i>
500 x 500 m	25	1	0.9978	0.9977	-0.0001
500 x 500 m	25	3	0.9978	0.9977	-0.0001
250 x 1000 m	25	1	0.9978	0.9973	-0.0005
250 x 1000 m	25	3	0.9978	0.9971	-0.0007
750 x 750 m	50	1	0.9666	0.9642	-0.0024
750 x 750 m	50	5	0.9666	0.9655	-0.0011

Stop forwarding DATA-messages

<i>Area size</i>	<i>Number of nodes</i>	<i>Baseline delivery rate</i>	<i>Delivery rate observed under attack</i>	<i>Delivery rate change</i>
500 x 500 m	25	0.9978	0.9973	-0.0005
250 x 1000 m	25	0.9978	0.9900	-0.0078
750 x 750 m	50	0.9666	0.9629	-0.0037

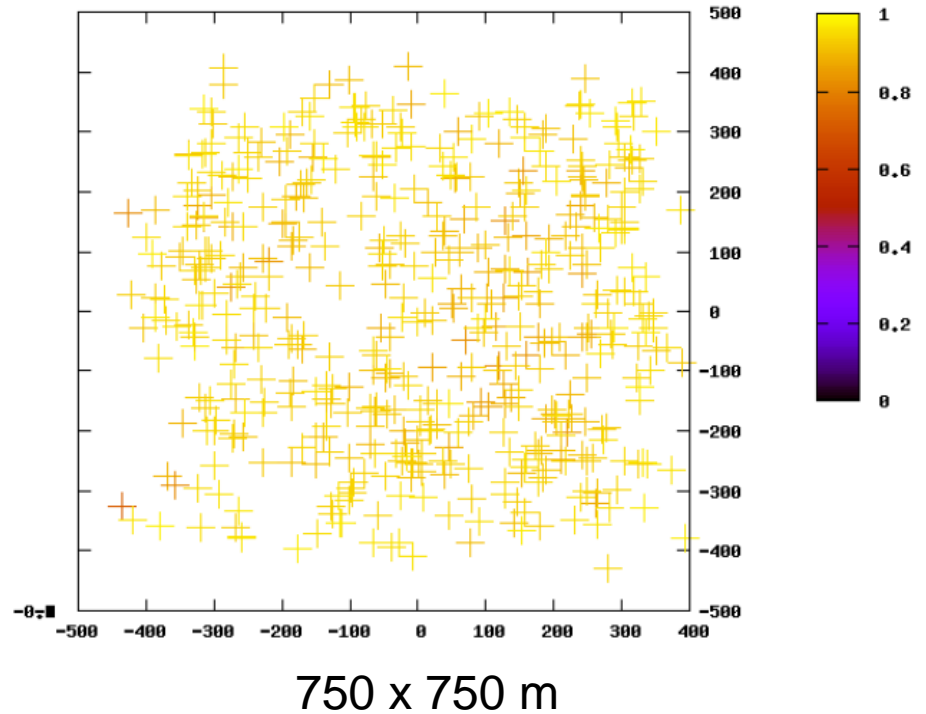
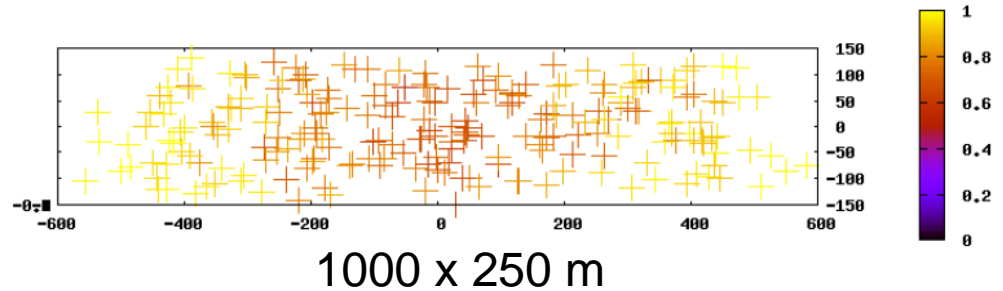
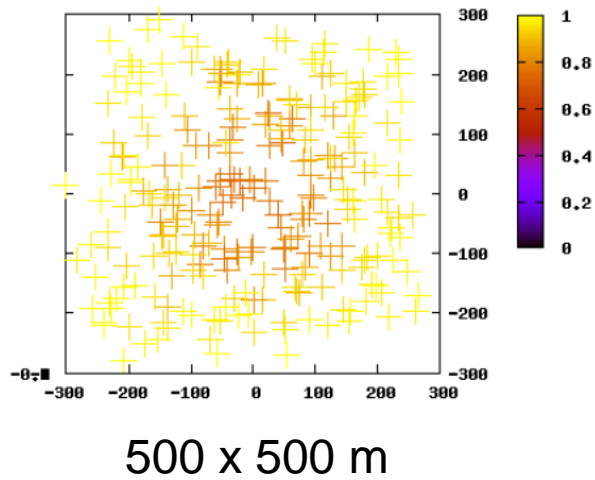
False ACK-messages based on network knowledge

<i>Area size</i>	<i>Number of nodes</i>	<i>Baseline delivery rate</i>	<i>Delivery rate observed under attack</i>	<i>Delivery rate change</i>
500 x 500 m	25	0.9978	0.8782	-0.1196
250 x 1000 m	25	0.9978	0.7815	-0.2163
750 x 750 m	50	0.9666	0.9268	-0.0398

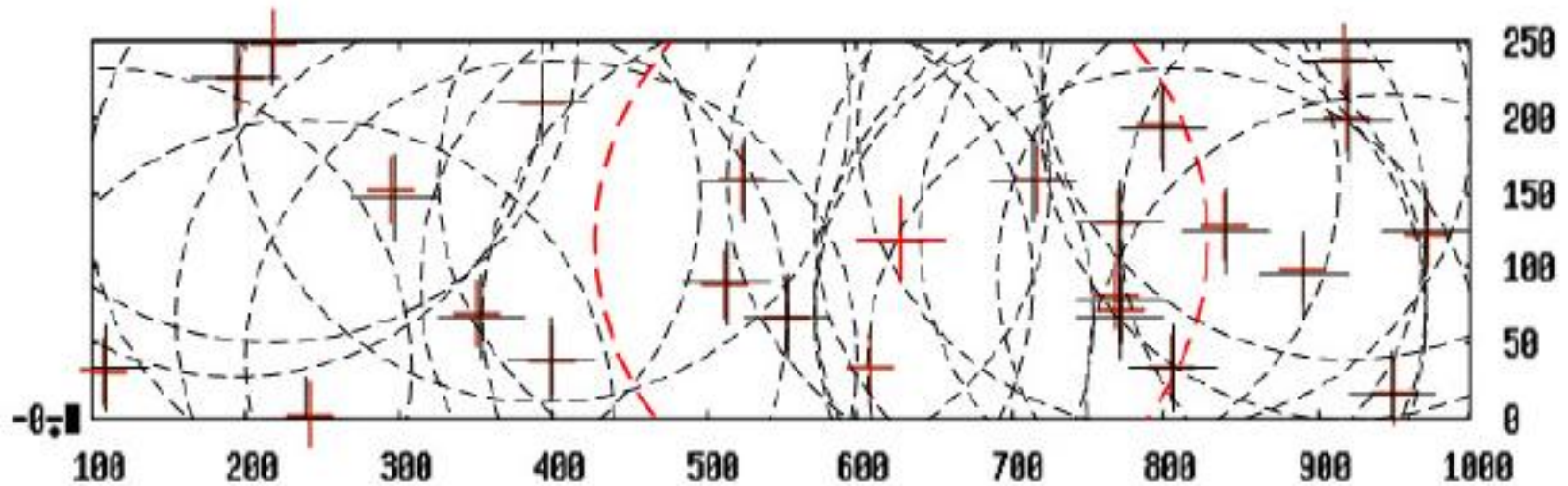
Many ACK-message attack

Area size	Number of nodes	Average	Mean	Standard derivation
500 x 500 m	25	0.8474	0.88135	0.1068
250 x 1000 m	25	0.7659	0.77375	0.1351

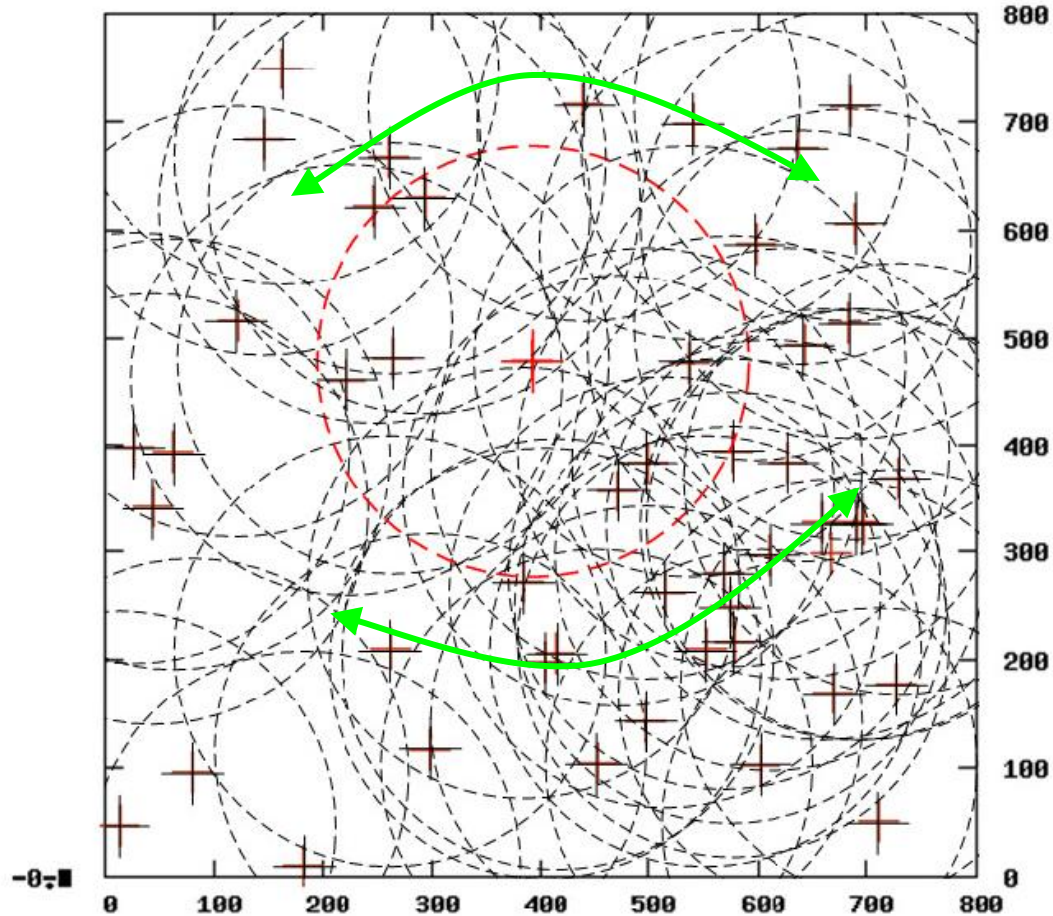
Attacker location analysis



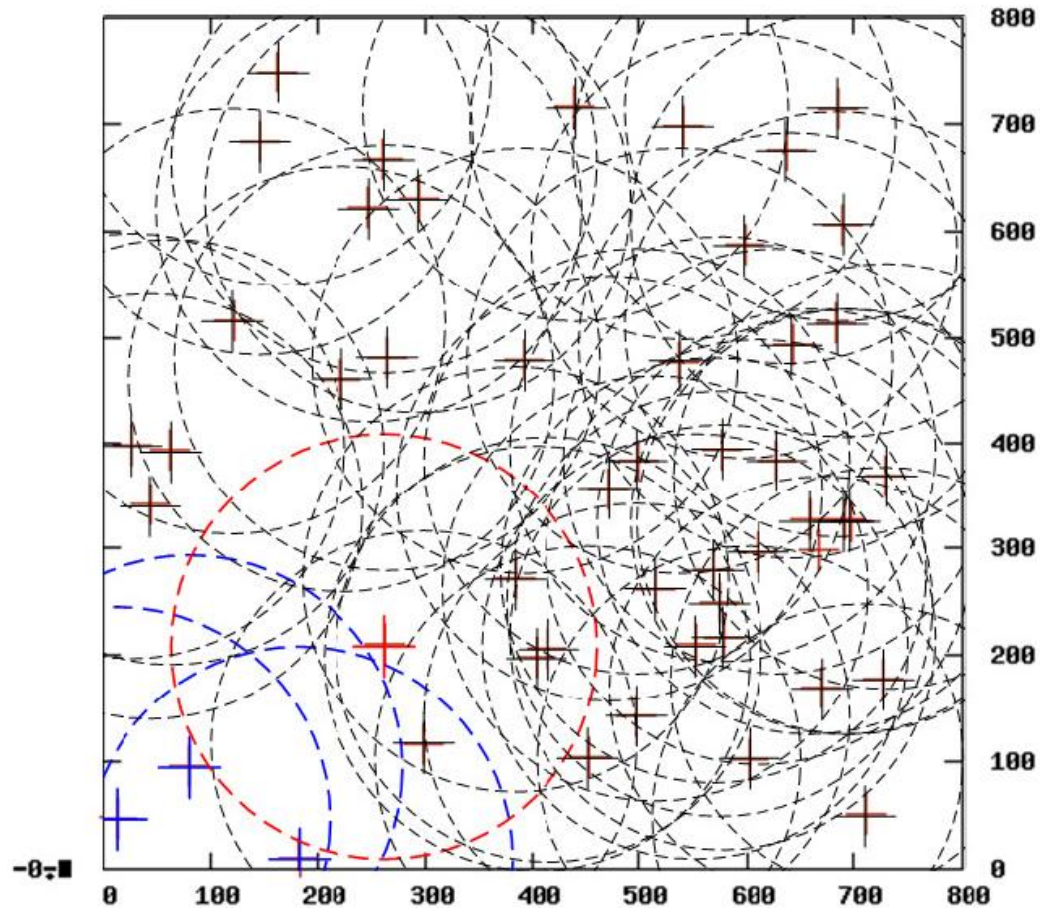
Attacker location analysis



Attacker location analysis



Attacker location analysis



False DATA-messages

<i>Area size</i>	<i>Number of nodes</i>	<i>Average</i>	<i>Mean</i>	<i>Standard derivation</i>
500 x 500 m	25	0.9956	0.9979	0.0075
250 x 1000 m	25	0.9939	0.99665	0.0092

- Why study publish/subscribe based MANET?
- Introduction to publish/subscribe networks
- Possible attacks on the protocol
- Presentation of findings
- **Protocol enhancements**
- Conclusion
- Questions

Public key cryptology

- Several attacks require the attacker to be able to impersonate other nodes
- Public key cryptology can be used to sign messages and verify the sender
 - Messages from attacker node will not be verified
 - Attacks will be stopped
- Message signing will however increase message size and resource required to handle each message
- Will not stop the “many ACK-message attack”

Keeping track of ACK-messages

- If we can keep track of which nodes has send ACK-message, we can stop attacking nodes from sending more than one ACK-message for each message
- Can be achieved by changing the ACK-count from an integer (counter) to a list of nodes, and remove nodes from list when ACK-message is received from node

<i>Area size</i>	<i>Number of nodes</i>	<i>Baseline delivery rate</i>	<i>Delivery rate when under attack with original protocol</i>	<i>Delivery rate when under attack with improved protocol</i>
500 x 500 m	25	0.9978	0.8474	0.9260
250 x 1000 m	25	0.9978	0.7738	0.9175

- Why study publish/subscribe based MANET?
- Introduction to publish/subscribe networks
- Possible attacks on the protocol
- Presentation of findings
- Protocol enhancements
- **Conclusion**
- Questions

Conclusion

- Publish/subscribe protocols are well suited for message distribution in ad-hoc networks
- We have shown how the publish/subscribe protocol proposed by Fongen is vulnerable to some attack types
- The proposed enhancements in the thesis can be used to make the protocol very intrusion tolerant against all attacks studied in the thesis

?