MSR: A Multipath Secure Reliable Routing Protocol for WSN

Presented by:
Mariam Ahmed Moustafa
elansary.mam@gmail.com

Faculty of Engineering, Alexandria University, Egypt
Mariam Ahmed Moustafa

- Is a talented Researcher, Teaching Assistant, Co-Founder of Dimensions Egypt. She received a Master of Science degree in Computer Science and Systems Engineering, Faculty of Engineering, Alexandria University, Egypt. She started her career as a Java software developer at ISFP (Integrated Solutions for Ports) for six years and IT Analyst at Unilever, then she joined the university as a teaching assistant for 6 semesters, after then she became the BlackBerry Developer Community Manager by developing dozens of top rated/paid mobile applications and games. In 2014, she establishes her own business as a software company called "Dimensions", which is specialized in developing 2D/3D and video games, mobile applications and Interactive architecture modeling. Mariam now is looking for applying to the next logical step in her life goals to be a PhD student.

- Mariam dream to make a big change in her society by typically model the Arab–African tech–women. She loves drawing. She can be contacted at: elansary.mam@gmail.com
MSR Publications


Objectives

1. Establish the need for secure routing in WSNs.
2. Present the main contributions of MSR scheme.
3. Analyze the proposed scheme and discuss the experimental results.
Agenda

- Introduction.
- Motivation.
- Scheme analysis.
- Experimental Results.
- Conclusion.
- References.
Recent advances in wireless communications have motivated the widespread of wireless sensor networks (WSNs), with the development of extremely small, low-cost, and low-power of multi functional sensor nodes.
WSNs market is growing worldwide. There is a drastic change in last few years and these number increases in future.
WSNs have attracted huge interest from the wireless research community due to their potential applications for both the military and civilian domains.
Introduction: WSNs Limitations

- Power restrictions.
- Storage restrictions.
- Limited computational power
- Lack of global IDs.
- Random deployment.
- Cooperative concept.
- The hostile and remote environment.
Motivation – Why Secure Routing?

- Communication **security** and reliability are two **important issues** in WSNs.
- WSNs possess a number of **additional security attacks**.
- **Infeasible** of using **traditional security solutions** like cryptography which requires complex processing to provide encryption to the transmitted data.
- **Lack of secure routing protocols**, many sensor network routing protocols have been proposed for WSNs, only few of them addressed secure routing.
- **Lightweight secure routing protocols should be addressed**.
Proposing a novel **MSR** secure routing protocol.

Utilizing **erasure coding** as a splitting method.

Utilizing **passive acknowledgment** as a security validation method.

Providing **security study** against major attacks.

Evaluating MSR scheme‘s performance.
MSR: A Multipath Secure Reliable Routing Protocol for WSNs

- On-Demand Multipath Routing
- Passive Acknowledgment
- Erasure Coding
Erasure coding is a forward error correction (FEC) code for the binary erasure channel, which transforms a message of $m$ blocks into a longer message with $n$ blocks (codeword) such that the original message can be reconstructed from a subset of the $n$ symbols. The fraction $r=m/n$ is called the code rate.
Passive Acknowledgment (PACK) refers to the sender passively listens after finishing the message transmission to confirm that the message has been received by the destination (indirect overhearing).
MSR: A Multipath Secure Reliable Routing Protocol for WSNs

- On-Demand Multipath Routing
- Passive Acknowledgment
- Erasure Coding
Security Analysis

**Security Attacks in WSNs:**
- Blackhole attack.
- Selective forwarding attack.
- Hello flood attack.
- Acknowledgment spoofing attack.
- Replay attack.
- Alter attack.
- Spoofing attack.
- Sinkhole attack.
- Wormhole attack.
- Sybil attack.
Security Analysis (cont.)

- **Security Attacks Definitions in WSNs:**
  - **Blackhole attack:** when a malicious node drops all the packets through it.
Selective forward attack: when a malicious node can however drop or forward certain messages (it selectively forward the packets).
Erasure coding provides an efficient option for achieving reliability against the noisy channel and efficient data replication without end-to-end retransmission.
Security Checks via Enhanced Passive Acknowledgment

- A consistent dropping of a packet from a neighbor can be used as a sign of a **blackhole** attack.
- A partial dropping of a packet from a neighbor can be used as a sign of a **selective forward** attack.
- Packet headers can be checked to detect any malicious changes in the headers. This can be used to detect **spoofing**.
- The packet content itself can be analyzed to detect any unauthorized changes to the packet. This can be used to detect **alter**.
Security Analysis (cont.)

MSR Defense Against Attacks

Attacks totally prevented
- Hello flood attack
- Blackhole attack
- Selective forwarding attack
- Acknowledgment spoofing attack

Attacks with reduced effect
- Replay, Alter, and Spoofing attacks
- Wormhole attack
- Sinkhole attack

Needs modifications
- Sybil attack
MSR protocol is implemented using NS–2 simulator. The main objective of the simulation is to evaluate the effectiveness of MSR relative to AOMDV (Ad hoc On-demand Multipath Distance Vector) which guarantees link-disjoint paths, doesn't use alternative paths simultaneously, uses retransmission concept for reliability and no security support.

Performance Metrics:
- Packet Delivery Ratio
- End-to-End Delay
- Normalized Routing Overhead
- Resistance against Attacks
Simulation parameters

Sensor nodes are spread randomly over a square area of dimensions 1000 * 1000 m$^2$. All experiments are performed against different network sizes (W) ranging from 50 to 200 sensor nodes.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>1000 sec</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>50, 100, 150 and 200</td>
</tr>
<tr>
<td>Network topology</td>
<td>1000*1000 m$^2$ square region</td>
</tr>
<tr>
<td>Traffic Source</td>
<td>CBR</td>
</tr>
<tr>
<td>Packet Size</td>
<td>1024 byte</td>
</tr>
<tr>
<td>Network Deployment</td>
<td>Random deployment</td>
</tr>
<tr>
<td>MAC Layer</td>
<td>MAC 802.11</td>
</tr>
<tr>
<td>Propagation Model</td>
<td>Two-Ray-Ground model</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Static</td>
</tr>
<tr>
<td>Seed</td>
<td>1, 3, and 7</td>
</tr>
</tbody>
</table>
Experimental Results (cont.)

- Simulation Setup
  - First Setup Experiment (effective sub-packet size)
  - Second Setup Experiment (effective coding rate)
Important parameters:

- **Packet size**: This parameter represents the size of the packets transmitted over the network.
- **Code rate**: This parameter represents the ratio of the total number of packets generated by the erasure coding technique to the sufficient number of packets to reconstruct the original message \((n/m)\).
Experimental Results (cont.)

- First Setup Experiment (effective sub-packet size)

Fig. 2. Effect of changing the sub-packet size on the performance of MSR.
Experimental Results (cont.)

- Second Setup Experiment (effective coding rate)

Fig. 3. Effect of changing the coding ratio on the performance of MSR.
**Experimental Results (cont.)**

- **MSR vs. AOMDV**
  - **Data Packet Delivery Ratio**
    - The results show that MSR outperforms AOMDV especially for small network sizes.
Experimental Results (cont.)

- MSR vs. AOMDV
  - **End-to-End Delay**
    - End-to-end delay is increased in MSR compared to AOMDV as MSR needs extra time to encode, send, decode and reconstruct the original message.

![Graph showing the comparison of End-to-End Delay for MSR and AOMDV]
MSR vs. AOMDV

- **Routing Overhead**
  - The results show that MSR has a slightly higher overhead compared to AOMDV.
Resistance against Attacks
  ◦ Against blackhole attack
    • MSR can achieve significant gain, more than 40%, as compared to AOMDV in the exist of blackhole attack.
Resistance against Attacks
  - **Against grayhole (selective forward) attack**
    - the selective forwarding attack is less severe than the blackhole attack as expected. As noticed the packet's delivery ratio improves while the dropping probability decreases in both protocols.
Analytical Analysis

Analytical Measures:

- $P_{os}$ → The successful delivery probability of a transmitted message.

- $P_{oq}$ → The successful delivery probability of a transmitted message if a malicious node can forward or drop a packet with probability.

- $M_{max}$ → The maximum number of attackers that MSR is resistant to ($= N - m$).
## Analytical Analysis (cont.)

### Analytical Parameters

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N$</td>
<td>Total number of disjoint routes.</td>
</tr>
<tr>
<td>$M$</td>
<td>Number of malicious routes due to nodes physical failure or certain attack.</td>
</tr>
<tr>
<td>$n$</td>
<td>Total number of erasure-coded packets.</td>
</tr>
<tr>
<td>$m$</td>
<td>Sufficient number of packets to reconstruct the original message.</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>Probability of a node to be malicious.</td>
</tr>
<tr>
<td>$\delta$</td>
<td>Number of hops or nodes per route.</td>
</tr>
<tr>
<td>$P_o$</td>
<td>The successful delivery probability of a transmitted message.</td>
</tr>
<tr>
<td>$P_{oq}$</td>
<td>The successful delivery probability of a transmitted message if a malicious node can forward or drop a packet with probability.</td>
</tr>
<tr>
<td>$M_{max}$</td>
<td>The maximum number of attackers that MSR is resistant to.</td>
</tr>
</tbody>
</table>
We can model the transmission of a packet on a route as a Bernoulli trials with successful probability \((1 - q)\) and unsuccessful probability \(q\).

\[
q = 1 - [(1 - \gamma)^\delta]
\]  

(5.1)

The successful delivery probability of sending block of packets per route \(P_{os}\).

\[
P_{os} = Pr(N - M \geq \frac{m}{s})
\]

(5.4)

\[
= \left\{ \begin{array}{cl}
\sum_{i=\frac{m}{s}}^{N} \binom{N}{i}(1-q)^i q^{N-i} , & N \geq \frac{m}{s}; \\
0 , & \text{otherwise}.
\end{array} \right.
\]

(5.5)
The probability $\hat{q}$ is that a malicious route has at least a malicious node and will not forward a packet with probability $\hat{q}$, then $P_{o\hat{q}}$ can be calculated as in Equation (5.6):

$$\hat{q} = 1 - [(1 - (\gamma \lambda))^\delta]$$  \hspace{1cm} (5.6)

Therefore $P_{o\hat{q}}$ can be calculated by replacing each unsuccessful probability $q$ with $\hat{q}$.

$$P_{o\hat{q}} = P_r(m \leq N - M) = P_r(N - M \geq m)$$

$$= \begin{cases} \sum_{i=m}^{N} \binom{N}{i}(1 - \hat{q})^i\hat{q}^{N-i}, & N \geq m; \\ 0, & \text{otherwise.} \end{cases}$$

$$\text{(5.7)} \hspace{1cm} (5.8)$$
MSR Complexity

- MSR route discovery algorithm is $O(bd)$ where,
  - $b$: number of a node’s neighbors
  - $d$: the max number of hops
- Erasure coding can be performed in a linear time as shown in [10, 11 and 12] then it adds $O(n)$.
  - $n$: the number of spitted shares.
- The security checks of PACK are performed simultaneously with the running of discovery with a constant magnitude, so the order still $O(K.bd)$ where, $K$: is constant.
- The total complexity of MSR is $O(K.bd) + O(n)$.
Conclusion

- On-Demand Multipath Routing
- Passive Acknowledgment
- Erasure Coding
Thank You

Questions
References


Related Work

- Recent advances in wireless sensor networks have led to many new protocols specially designed for but few of them consider security.
- H–SPREAD[2], MDR[3], SMR[4] and AOMDV[1].
- We focus on AOMDV (Ad hoc On–demand Multipath Distance Vector), it guarantees loop freedom and link–disjoint paths.
- Back draws of AOMDV:
  - Doesn’t use alternative paths simultaneously.
  - Use retransmission concept for reliability.
  - No Security support.
Future Work

- Approve the simulation results analytically.
- MSR against difficult attacks and environmental conditions.
  - Sybil and mobile/energy-aware.
- MSR performance optimization.
  - Use efficient routing metrics.
- MSR packet allocation optimization.
  - Weighted-k-out-of-n algorithm.
The sensor network is static.
The sensor nodes are homogeneous.
The communication channels are bidirectional.
The deployment is random.
**MSR: On-Demand Multipath Routing (cont.)**

**ROUTE_REQUEST packet format**

<table>
<thead>
<tr>
<th>sourceId</th>
<th>destinationId</th>
<th>requestId</th>
<th>hopCount</th>
<th>...</th>
</tr>
</thead>
</table>

**sourceId:** the Id of the source node that originated the ROUTE_REQUEST.

**destinationId:** the Id of the destination node for which the route is desired.

**requestId:** a sequence number uniquely identifying the particular ROUTE_REQUEST when taken in conjunction with the sourceId and the destinationId.

**hopCount:** the number of hops from source node to the node handling the request.
**MSR: On-Demand Multipath Routing (cont.)**

**ROUTE_REPLY packet format**

<table>
<thead>
<tr>
<th>sourceId</th>
<th>destinationId</th>
<th>requestId</th>
<th>hopCount</th>
<th>lifeTime</th>
<th>timeOut</th>
<th>...</th>
</tr>
</thead>
</table>

- **sourceId**: the Id of the source node that originated the ROUTE_REQUEST.
- **destinationId**: the Id of the destination node for which the route is desired.
- **requestId**: a sequence number uniquely identifying the particular ROUTE_REQUEST when taken in conjunction with the sourceId and the destinationId.
- **hopCount**: the number of hops from source node to the node handling the request.
- **lifeTime**: the time for which nodes receiving the ROUTE REQUEST consider the route to be valid.
- **timeOut**: the time to discover the multipaths, starts from the arrival of the first ROUTE REPLY and waiting for this timeOut period to stop receiving any extra replies.
MSR: On-Demand Multipath Routing (cont.)

Routing Discovery Algorithm

Lifetime

Timeout

Fresh Path

ROUTE_REQ UEST

ROUTE_REPLY
The on-demand multipath route discovery process as follows:

- When a node needs a route to a destination, it broadcasts a ROUTE-REQUEST.
- Any node with a current route to that destination, can unicast a ROUTE-REPLY back to the source node.
- Route information is maintained by each node in its routing table.
- Information obtained through ROUTE-REQUEST and ROUTE-REPLY packets is kept with other routing information in the route table.
Erasure coding provides an efficient option for achieving reliability against the noisy channel and efficient data replication without end-to-end retransmission [16].
In erasure coding, selecting an optimal value of the encoding code rate $r$, where $r = \frac{n}{m}$, is a critical issue. In general the larger it is, the more reliability we can achieve but with the more overhead as well.
Security Check via Enhanced Passive Acknowledgment

- A consistent dropping of a packet from a neighbor can be used as a sign of a **blackhole** attack [23].
- A partial dropping of a packet from a neighbor can be used as a sign of a **selective forward** attack [23].
- Packet headers can be checked to detect any malicious changes in the headers. This can be used to detect **spoofing**.
- The packet content itself can be analyzed to detect any **unauthorized changes** to the packet.
Introduction.
Motivation.
Contribution.
Background.
Related Work.
Scheme analysis.
Experimental Results.
Conclusions.
Future Work.
Objectives Review.
References.
Background

- Security requirements.
- Attacker models.
  - Erasure coding.
  - Passive acknowledgment.
Background – Security Requirements

- Authentication.
- Availability.
- Confidentiality.
- Integrity.
- Freshness.
Background – Attacker Models

- Mote-class versus laptop-class.
- Passive versus active.
- Outsider versus insider.
Erasure coding is a forward error correction (FEC) code for the binary erasure channel, which transforms a message of \( m \) blocks into a longer message with \( n \) blocks (codeword) such that the original message can be reconstructed from a subset of the \( n \) symbols. The fraction \( r = m/n \) is called the code rate.
Passive Acknowledgment (PACK) refers to the sender passively listening after finishing the message transmission to confirm that the message has been received by the destination (indirect overhearing).
The network is static.
The sensor nodes are homogeneous.
The communication channels are bidirectional.
The deployment is random
Each sensor node has a unique Id.
An attacker is assumed to be a mote–class, insider, and active.
Security Analysis

Security Attacks Definitions in WSNs:

- **Hello flood attack**: a laptop-class adversary broadcasting routing information with large transmission power could convince every node in the network that the adversary is its neighbor.
Security Analysis (cont.)

- **Security Attacks Definitions in WSNs:**
  - **Blackhole attack:** when a malicious node drops all the packets through it.
Security Attacks Definitions in WSNs:

- **Selective forward attack**: when a malicious node can however drop or forward certain messages (it selectively forward the packets).
Security Analysis (cont.)

- **Security Attacks Definitions in WSNs:**

- **Acknowledgment spoofing attack:** when a malicious node spoofs an acknowledgment convincing the sender that a weak link may be strong or a dead node is alive.
Security Attacks Definitions in WSNs:

Replay, alter and spoofing attacks: Adversaries are retransmitted the valid data repeatedly to inject the network routing traffic. They may be able to attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency.
Security Analysis (cont.)

- **Security Attacks Definitions in WSNs:**

- **Sinkhole attack:** An adversary tries to attract almost all the traffic toward the compromised node. (The path presented through the malicious node appears to be the best available route for the nodes to communicate)
Security Analysis (cont.)

- **Security Attacks Definitions in WSNs:**

- **Wormhole attack:** An adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed. (Wormholes are dangerous because they can do damage without even knowing the network.)
Security Analysis (cont.)

- **Security Attacks Definitions in WSNs:**

- **Sybil attack:** a single adversary node presents multiple identities to all other nodes in the WSN, which may affect data aggregation, voting or disjoint path routing.