Source of Figure: http://trust.csu.edu.cn/conference/trustcom2008/

Trusting Anomaly and Intrusion Claims for Cooperate Distributed Intrusion Detection Schemes of Wireless Sensor Networks

Presented by:

Riaz Ahmed Shaikh

Date: 19th November 2008

Ubiquitous Computing Lab, Kyung Hee University, Korea

http://uclab.khu.ac.kr/usec/riaz

Email: riaz@khu.ac.kr

Agenda

- Background and Motivation
- Problem Description
- Related Work
- Network and Adversary Model
- Definitions and Assumptions
- Algorithm description
- Analysis and Evaluation
- Conclusion and Future Work

Background and Motivation

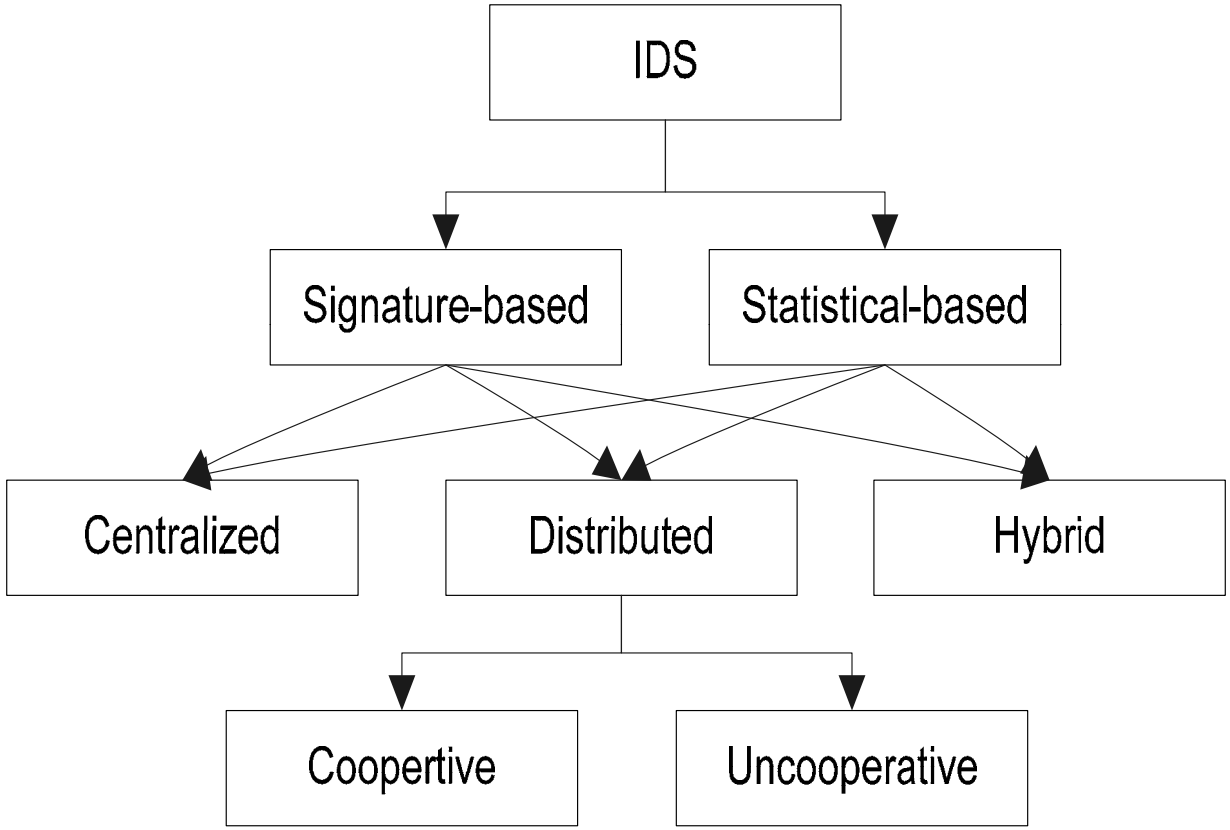
- Many anomaly and intrusion detection schemes have been proposed for WSNs, but those schemes mainly focuses on the detection of a malicious or faulty node(s).

- All those anomalies and IDS schemes that are cooperative in nature needs to share anomalies or intrusions claims. However those schemes are unable to provide assurance that the report or claim received by the other node(s) is really send by the trusted node(s).

Problem Statement

- Any unidentified malicious node(s) in the network could send faulty anomaly and intrusion claims about the legitimate node(s) to the cluster head, base station or any other specific sink node(s). Verifying the validity of those claims is a challenging and critical issue that remains unsolved for WSNs.

Related Work: Taxonomy

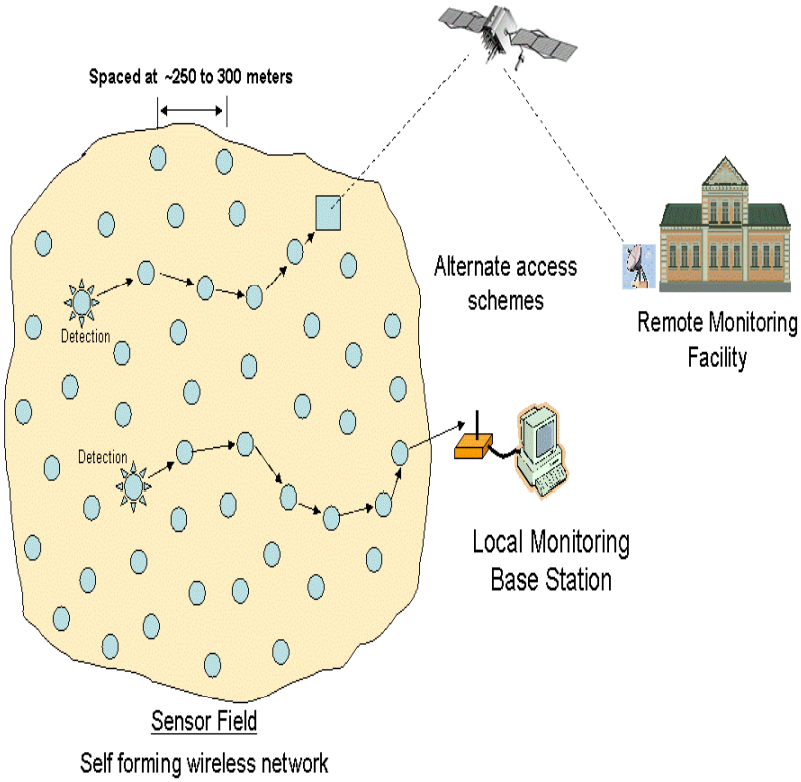


Related Work:
Classification and Comparison of Existing Schemes

		V. Bhuse et al. [1]	W. Du et al. [2]	C. E. Loo et al. [3]	V. Chatzigiannakis et al. [4]	A. P. R. da Silva et al. [5]
Classification	IDS technique	Signature-based	Statistical-based	Statistical-based	Statistical-based	Statistical-based
	IDS architecture	Distributed & cooperative	Distributed & cooperative	Distributed & uncooperative	Hybrid	Distributed & uncooperative
Specifications	Installation of IDS	On every sensor node	On every sensor node	On every sensor node	On every primary node (Cluster head) of a group	Special monitor sensor nodes in the network
	IDS Scope	Multilayer (Appl., Net., MAC & Phy.)	Application layer	Network Layer	Application layer	Multilayer (Appl., Net., MAC & Phy.)
	Attacks detects	Masquerade attack, and forged packets attacks	Localization anomalies	Routing attacks (e.g. Periodic error route attack, active & passive sinkhole attack)	Correlated anomalies/ attacks (invalid data insertion)	Worm holes, data alteration, Black hole, selective forwarding, & jamming
Environment	Sensor nodes	Static /Mobile	Static	Static /Mobile	Static /Mobile	Static
	Topology	Any	Any	Any	Cluster-based	Tree-based

Network Model

- Sensor nodes are deployed in an environment either in a random fashion or in a grid fashion,
  - which are organized in any form of topology (e.g. cluster-based etc).
    - Any data-centric (e.g. directed diffusion etc) or address-centric (e.g. AODV etc) routing scheme could be used.



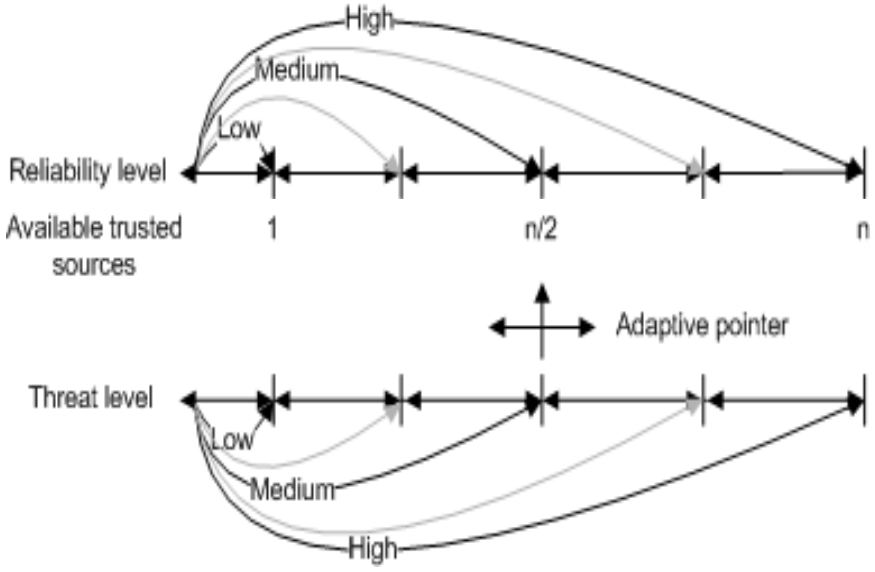
http://www.alicosystems.com/Wireless%20Sensor%20Networks.gif

Adversary Model

- A legitimate node which is compromised by an adversary is called a malicious node.
- So the malicious node could performed malicious activities like dropping and fabrication of packets etc.
- Also in order to hide the presence of the adversary, a malicious node could also perform all the activities like normal nodes do such as monitoring, ciphering of data, forwarding of packets etc.

Approach and Definitions

- Reliability can be simply categorized into three basic levels: Low, Medium, and High.
  1. In the low reliability mode, validation is based on the confirmation from any one available reliable source.
  2. In the medium reliability mode, validation is based on the confirmation from half of the available reliable sources.
  3. In the high reliability mode, validation is based on the confirmation from all of the reliable sources.



In order to achieve more flexibility and adaptability, we introduce intrusion-aware reliability mode concept, in which validation reliability is based on the level of threat of anomaly or intrusion.

Assumptions

- Any cooperative-based distributed anomaly or IDS is already deployed in the WSNs, which forward claim(s) to the other node(s) whenever it detects some anomalies or intrusions.
- The malicious node must fall into the radio range of the monitoring node. And the node (who received the claim from the monitoring node) has the knowledge about the neighboring nodes of the monitoring and malicious nodes.
- We have also assumed that the multiple sensor nodes in a neighborhood can sense the same anomaly/intrusion.
- We also assumed that all information is exchanged in a secure encrypted manner.

Algorithm: Phase 1 (Consensus Phase)

1. Whenever a designated node received a claim packet (Line 1) which includes the information about the identities of the sender & malicious nodes and specific details about the anomaly and intrusion, it will first checks whether the identity of a new malicious node is already declare as a malicious node or not (Line 2).

2. If not then the node will first get the common neighborhood list of the sender and malicious nodes respectively. After that the node will eliminate any known malicious node(s) from that list(Line 3:6).

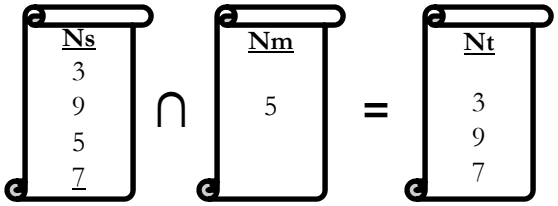
3. Then based on the threat level, confirmation request packet(s) is forwarded to the randomly selected node(s) from the N_t list (Line 7:19).
   - For example, if the threat is of medium level, then the confirmation request packets are forwarded to the half of the randomly selected nodes from the list N_t (Line 10:13).

4. If the information about the malicious node is already present (line 20) then the node will just update its old record (Line 21).

Algorithm III.1 Phase 1: Consensus Phase

```
1: Received Claim Packet Pkt (ID_sender, ID_mal,detail);
2: if ID_mal is new then
3:    N_s = GetNeighorList(ID_sender);
4:    N_m = GetNeighorList(ID_mal);
5:    N_sm = N_s ⋂ N_s;
6:    N_t = Eliminate-Known-Malicious-Nodes(N_sm);
7:    if N_t ≠ φ then
8:       if ThreatLevel(detail) is Low then
9:          Send Conf-Req-Pkt(Rand(N_t), ID_mal,detail);
10:      else if ThreatLevel(detail) is Medium then
11:         for i = 1 to len(N_t)/2 do
12:            Send Conf-Req-Pkt(Rand(N_t), ID_mal,detail);
13:         end for
14:      else
15:         for i = 1 to len(N_t) do
16:            Send Conf-Req-Pkt(ID_i, ID_mal,detail);
17:         end for
18:      end if
19:   end if
20: else
21:    Update Record;
22: end if
```

Algorithm: Phase 1 (Consensus Phase)

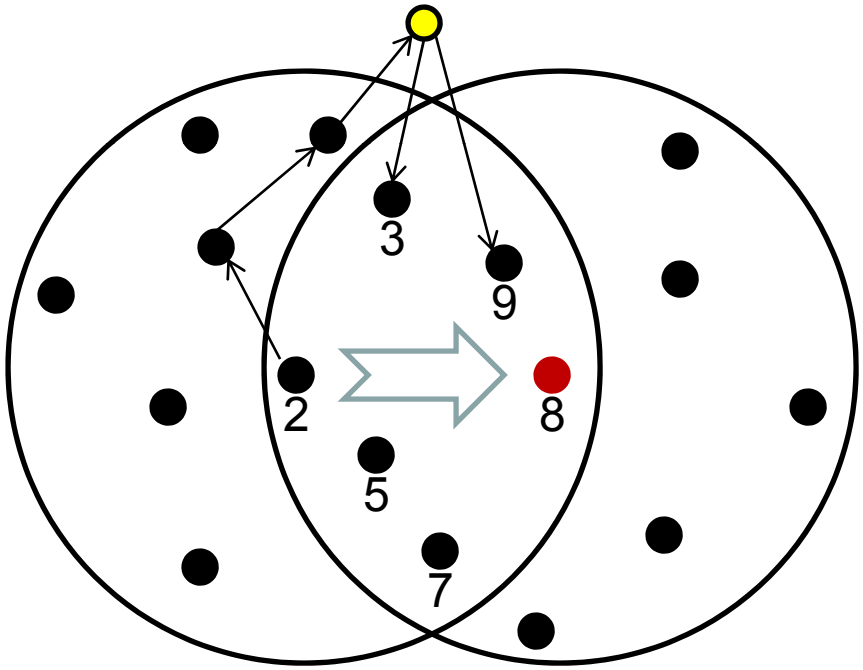


3	8	M_{code}

conf-req-pkt

9	8	M_{code}

conf-req-pkt



2	8	M_{code}

Claim packet

Algorithm: Phase 2 (Decision Phase)

In this phase, algorithm will first wait for the confirmation response packets until Δt *time:*

$$\Delta t = 2\left[2t_{prop} + t_{proc}\right]$$

A node will expect three types of responses *r* from each node who received confirmation request packets:

$$r_{i,j} = \begin{cases} 1 & if \quad agree\,with\,claim \\ 0 & if \quad don't\,know \\ -1 & if \quad not\,agree\,with\,claim \end{cases}$$

A node *i* will make the decision (*D*) about the validity and invalidity of the claim based on a following rule:

$$D_i = \begin{cases} validate & iff \quad \sum_{j=0}^{n_{res}} r_{i,j} > 0 \\ invalidate & iff \quad \sum_{j=0}^{n_{res}} r_{i,j} < 0 \\ no\,consensus & iff \quad \sum_{j=0}^{n_{res}} r_{i,j} = 0 \end{cases}$$

If no consensus builds then the algorithm will make the decision best on its mode that is set by the administrator. There are two types of modes: aggressive and defensive. If algorithm is set as an aggressive mode then the node will validate the claim and vice versa.

Reliability Analysis

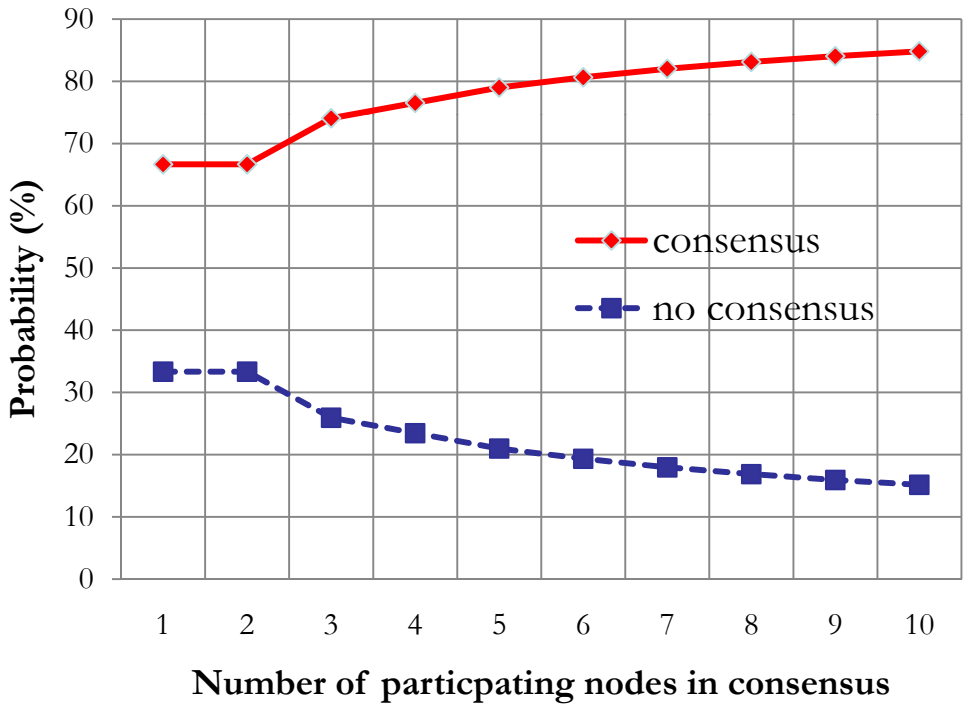
For uniform distribution

$$P_c = \frac{N_c}{K^{n_{res}}}$$

For other distributions

$$P_c = \sum_{m=1}^{M} (\Pi_{i=1}^{n_{res}} PMF_i(S_m(i))) \times \delta(m), \quad M = K^{n_{res}}$$

N_c : # of nodes reaching at consensus.
K : # of possible outcomes.
n_{res} : # of responses received
δ(m) : is 1 if m nodes reaches consensus otherwise 0.
PMFi : probability mass function that captures the probability distribution of the symbol produced by the node *i.*
Sm(i): *is the i^{th} symbol in the m^{th}* node result.



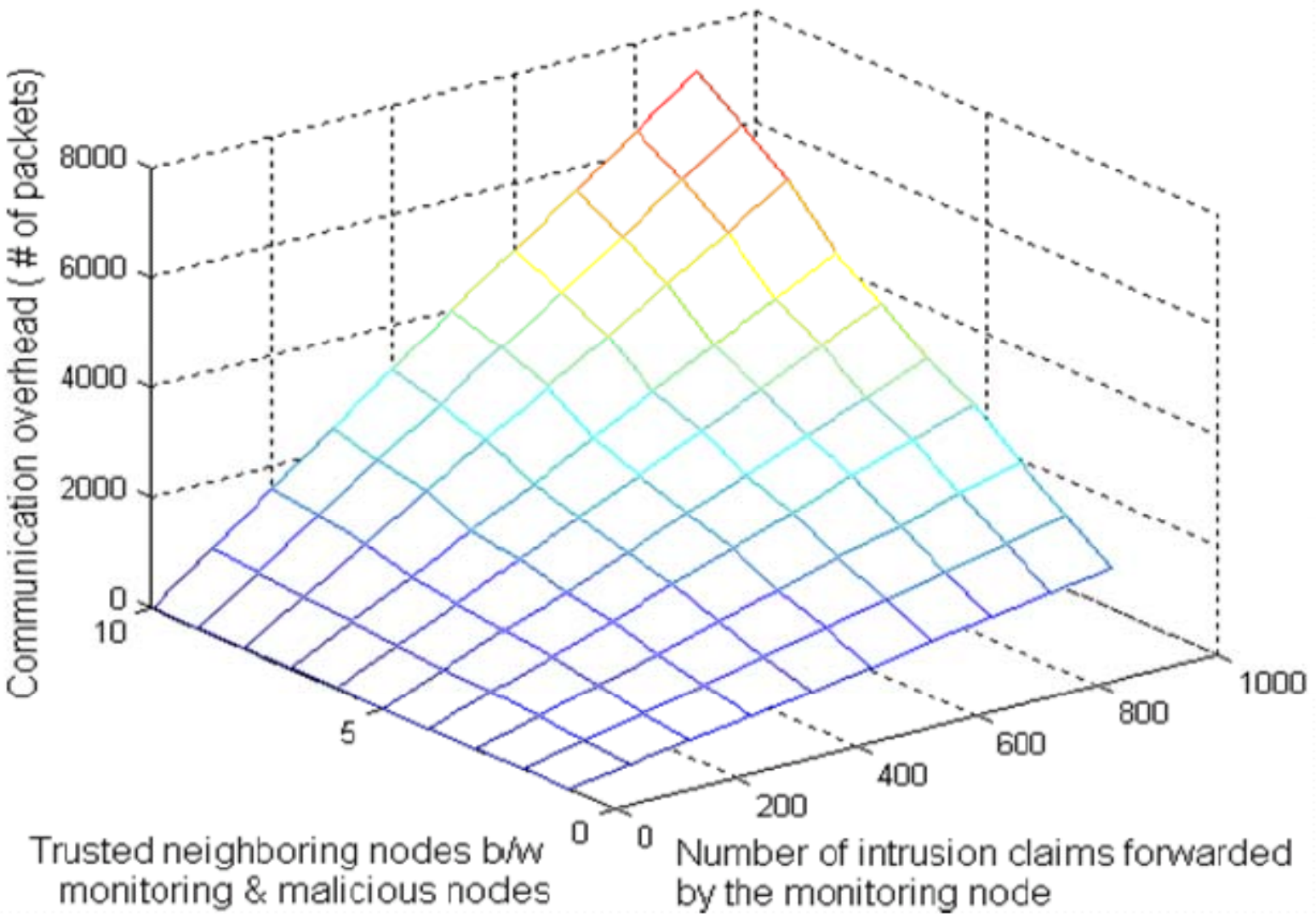
Communication Overhead Analysis

- Communication overhead of the validation algorithm is depended on three factors:
  1. Total number of intrusion claims *(Ic),*
  2. Number of common trusted neighboring nodes, and
  3. Threat level of intrusion or anomaly.

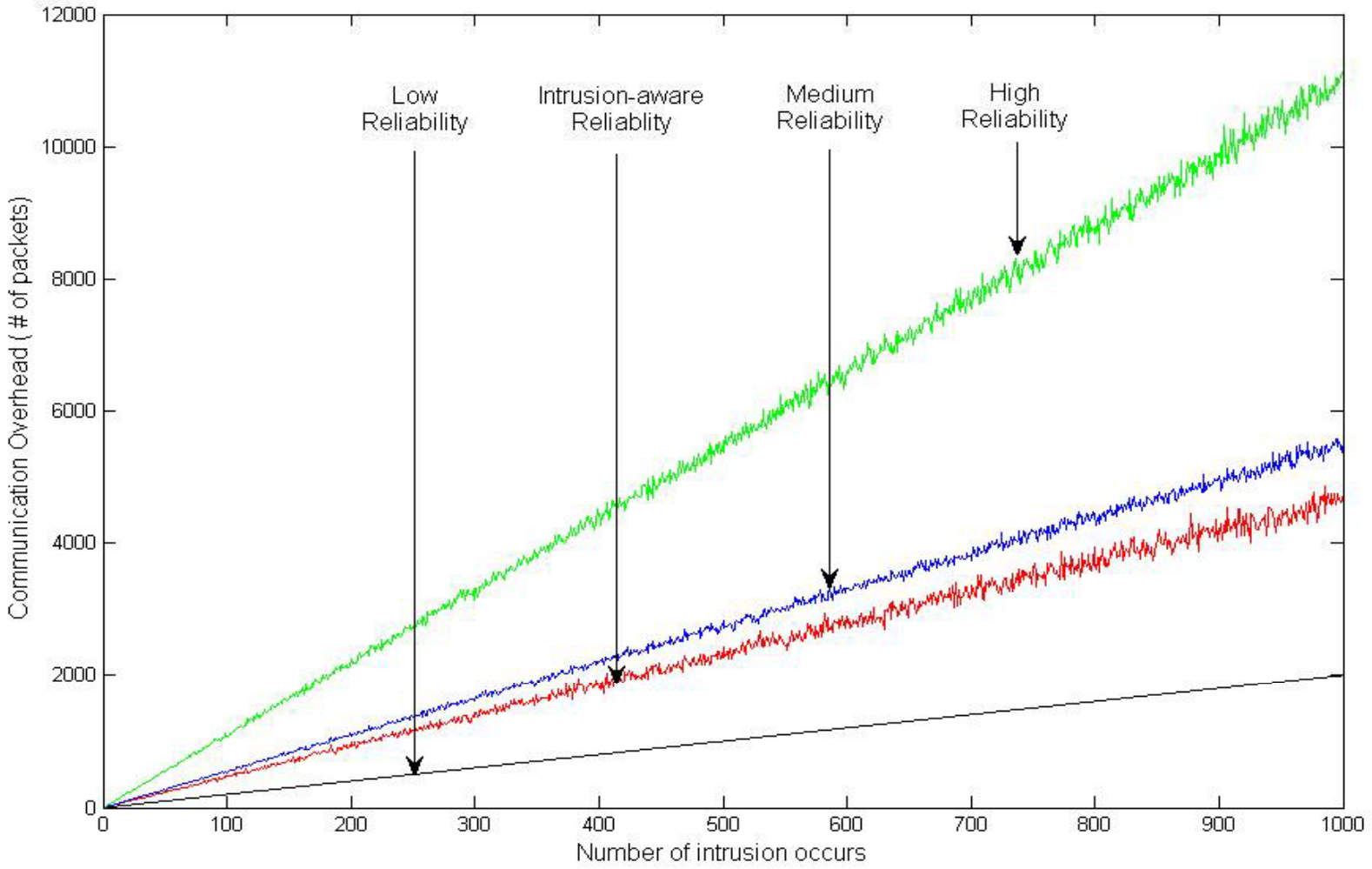
	Cost
Low Reliability	$2\ I_c$
Medium Reliability	$m_t I_c$
High Reliability	$2m_t I_c$
Intrusion-aware Reliability	$2I_c + (I_m + 2I_h)\ m_t$

- Here, m_t represents the average number of common trusted neighboring nodes, and
- $I_c = I_l + I_m + I_h$

Communication Overhead Analysis



Communication Overhead Analysis



Conclusion

- Existing cooperative-based anomaly and intrusion detection schemes of WSNs does not provide assurance that the reports or claims received by the other node(s) are really send by the trusted legitimate node(s).

- Therefore, in this work we have proposed first validation algorithm for trusting anomalies and intrusion claims.

- This algorithm uses the concept of intrusion-aware reliability parameter that helps to provide adequate reliability at the modest cost of communication.

Future work

- The proposed work is still in preliminary stage and is based on a few strict assumptions, such as multiple nodes can sense same anomaly/intrusion.

- In practical, it is quite possible that only one node can detect some specific anomaly/intrusion. In this case, our scheme will not be able to validate the claim.

- Algorithm should also needed to be evaluate from the security resiliency perspective.

References

1. V. Bhuse, and A. Gupta, "Anomaly intrusion detection in wireless sensor networks", Journal of High Speed Networks, vol. 15, pp. 33-51, 2006

2. W. Du, L. Fang, and N. Peng, "LAD: Localization anomaly detection for wireless sensor networks", Journal of Parallel and Distributed Computing, vol. 66, pp. 874-886, 2006

3. C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion Detection for Routing Attacks in Sensor Networks", Int. Journal of Distributed Sensor Networks, vol. 2, pp. 313-332, 2006

4. V. Chatzigiannakis, S. Papavassiliou, "Diagnosing Anomalies and Identifying Faulty Nodes in Sensor Networks", IEEE Sensors Journal, vol. 7(5), pp. 637-645, 2007

5. A. P. R. da Silva, M. H.T. Martins, B. P.S. Rocha, A.A.F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks", Proc. of the 1st ACM Int. workshop on Q2SWinet, Oct 2005, Canada , pp. 16-23