A CLUSTER BASED METHOD FOR REDUNDANCY MANAGEMENT IN WIRELESS SENSOR NETWORKS

T. Mallikadevi [1] J.Pushpa kumara [2] K.Krushnaveni [3]
Assistant Professors,
Department of CSE
Narsimha Reddy Engineering College, Maisammaguda, Dhulapally,
Kompally, Secunderabad – 500 100

ABSTRACT

In this paper, we contend tautology management of diversified wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malevolent nodes. The key concept of our tautology management is to exploit the tradeoff between energy consumption vs. the gain in trustee worthiness, well timed, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best tautology level to apply to multipath routing for intrusion endurance so that the query response success contigency is maximized while prolonging the useful lifetime. Furthermore, we consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malevolent nodes in a diversified wireless networks.

Keywords: Tautology, Diversified Wireless Sensor Networks, Distributed Intrusion,

1. INTRODUCTION

Most of the wireless sensor networks (WSNs) are deployed in an unattended environment in which energy replenishment is difficult if not impossible. Due to limited resources, a WSN must not only satisfy the application specific QoS requirements such as trustworthiness, timeliness and security, but also minimize energy consumption to prolong the system useful lifetime. The tradeoff between energy consumption vs. trustworthiness gain with the goal to maximize the WSN system lifetime has been well explored in the literature. However, no prior work exists to consider the tradeoff in the presence of malevolent attackers. It is commonly believed in the research community that clustering is an effective solution for achieving scalability, energy conservation, and trustworthiness.

Multipath routing is considered an effective mechanism for fault and intrusion endurance to improve data delivery in WSNs. The basic idea is that the contigency of at least one path reaching the sink node or base station increases as we have more paths doing data delivery.

2. RELATED WORK

Over the past few years, many protocols exploring the trade- off between energy consumption and QoS gain particularly in trustworthiness in HWSNs have been proposed. In [15], the optimal communication range and communication mode were derived to maximize the HWSN lifetime. In [16], the authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a hierarchal HWSN with CH nodes having larger energy and processing capabilities than normal SNs. The solution is formulated as an optimization problem to balance energy consumption across all nodes with their roles. In either work cited above, no consideration was given to the existence of malevolent nodes.

Over the past few years, numerous protocols have been proposed to detect intrusion in WSNs. [7], [11] provide excellent surveys of the subject. In [10], a decentralized rule- based intrusion detection system is proposed by which monitor nodes are responsible for monitoring neighboring nodes. The monitor nodes apply predefined rules to collect messages and raise alarms if the number of failures exceeds a threshold value. Our host IDS essentially follows this strategy, with the flaws of the host IDS characterized by a false positive contigency ($Hpf\,p$) and a false negative contigency ($Hpf\,n$). One approach especially applicable to flat WSNs is for an intermediate node to feedback malevolentness and energy status of its neighbor nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable malevolentness or energy status .Another approach which we adopt in this paper is to use local host-based IDS for energy conservation (with SNs monitoring neighbor SNs and CHs monitoring neighbor CHs only), coupled with voting to cope with node collusion for implementing IDS functions (as discussed in Section III in the paper).

3. SYSTEM MODEL

A HWSN comprises sensors of different capabilities. We consider two types of sensors: CHs and SNs. CHs are superior to SNs in energy and computational resources.

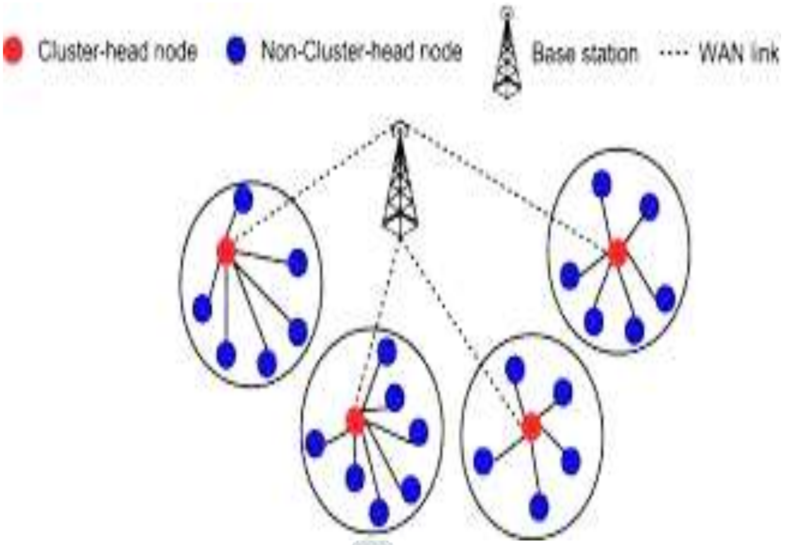


Fig. 1: Source and path redundancy for a heterogeneous WSN

All sensors are subject to capture attacks, i.e., they are vulnerable to physical capture by the adversary after which their code is compromised and they become inside attackers. Due to limited resources, we assume that when a node is compromised, it only performs two most energy conserving attacks, namely, bad-mouthing attacks (recommending a good node as a bad node and a bad node as a good node)

Redundancy management of multipath routing for intrusion endurance is achieved through two forms of redundancy: (a) source redundancy by which m_s SNs sensing a physical phenomenon in the same feature zone are used to forward sensing data to their CH (referred to as the source CH); (b) path redundancy by which m_p paths are used to relay packets from the source CH to the PC through intermediate CHs. Fig. 1 shows a scenario with a source redundancy of 3 ($m_s = 3$) and a path redundancy of 2 ($m_p = 2$).

To preserve confidentiality, we assume that the HWSN executes a pair wise key establishment protocol in a secure interval after deployment. Each node establishes pair wise keys with its *k*-hop neighbors, where *k* is large enough to cover a cluster area. Thus, when SNs join a new cluster, the CH node will have pair wise keys with the SNs joining its cluster. Since every SN shares a pair wise key with its CH, a SN can encrypt data sent to the CH for confidentiality and authentication purposes. Every CH also creates a pair wise key with every other CH.

Symbol	Meaning	Type
A	Length of each side of a square sensor area (meter)	Input
Nb	Size of a data packet (bit)	Input
Eelec	Energy dissipation to run the transmitter and receiver circuitry (J/bit)	Input
Eamp	Energy used by the transmit amplifier to achieve an acceptable signal to	Input
Eo	Initial energy per node (Joule)	Input
Einit	Initial energy of the HWSN (Joule)	Derived
Eclustering(t)	Energy consumed for executing the clustering algorithm at time *t* (Joule)	Derived
EIDS(t)	Energy consumed for executing the IDS algorithm at time *t* (Joule)	Input
Eq(t)	Energy consumed for executing a query at time *t* (Joule)	Derived
Rq(t)	Contigency that a query reply at time *t* is delivered successfully by the	Derived

R	Wireless radio communication range (meter)	Input
Q	node hardware failure contigency	Input
Ej	Transmission failure contigency of node *j*	Input
N(t)	Number of nodes in the HWSN at time *t*	Input
sNCH(t)	Number of CHs in the HWSN at time *t*	Derived
NSN(t)	Number of SNs in the HWSN at time *t*	Derived
n(t)	Number of neighbor nodes at time *t*	Derived
ngood(t)	Number of good neighbor nodes at time *t*	Derived
nbad(t)	Number of bad neighbor nodes at time *t*	Derived
Nq	Maximum number of queries before energy exhaustion	Derived
Mp	Path redundancy level: Number of paths from a source CH to the sink	Design
Ms	Source redundancy level: Number of SNs per cluster in response to a	Design
F	Fraction of neighbor nodes that will forward data	Input
$\lambda(t)$	Node population density (nodes/meter^2) at time *t*	Derived
Λ	Node population density at deployment time	Input

4. CONTIGENCY MODEL

In this section, we develop a contingency model to estimate the MTTF of a HWSN using multipath data forwarding to answer queries issued from a mobile user roaming in the HWSN area. Table I provides the notation used for symbols and their physical meanings. We use the same notation for both CHs and SNs, e.g., Pfp and Pfn. SN. A parameter is labeled as *input*, derived, design or output.

The basic idea of our MTTF formulation is that we first deduce the maximum number of queries, Nq, the system can possible handle before running into energy exhaustion for the best case in which all queries are processed successfully. Because the system evolves dynamically, the amount of energy spent per query also varies dynamically.

A. Network dynamics:

Initially, at deployment time all nodes (CHs or SNs) are good nodes. Then, the contingency that a SN is compromised at time t, given that it was a good node at time $t-TIDS$, denoted by Pc, is given by:

$$P_c=1-P\{X>t|X>t-T_{rds}\}$$

We note that Pc is time dependent. For the special case in which the capture time is exponential distributed with rate $\ddot{e}c$, $Pc = 1-e^{-\ddot{e}c \times TIDS}$. At the i^{th} IDS execution time (denoted by tI,i), a good node may have been compromised with contigency Pc since the previous IDS execution time ($tI,i-1$). Let $ngood\ (t)$ and $nbad\ (t)$ denote the numbers of good and bad neighbor nodes at time t, respectively, with $ngood\ (t) + nbad\ (t) = n\ (t)$. Then, the population of good and bad neighbor nodes at time tI,i just prior to IDS execution can be recursively estimated from the population of good and bad neighbor nodes at time $tI,i-1$ as follows:

$$ngood\,(tI,i) \quad = \quad ngood\,(tI,i-1) - ngood\,(tI,i-1) \times Pc \quad nbad\,(tI,i) \quad = nbad(tI,i-1) +$$

$$n_{good}(t_{I,i}-1)\times P_{c}\text{-(4)}$$

B. Query success contingency:

The first source of failure, transmission speed violation, accounts for query deadline violation. To know the failure contingency due to transmission speed violation, we first derive the minimum hop-by-hop transmission speed required to satisfy the query deadline T_{req}. Let d_{SN-CH} be expected distance between a SN and its CH and d CH-PC be the expected distance between the source CH and the PC.

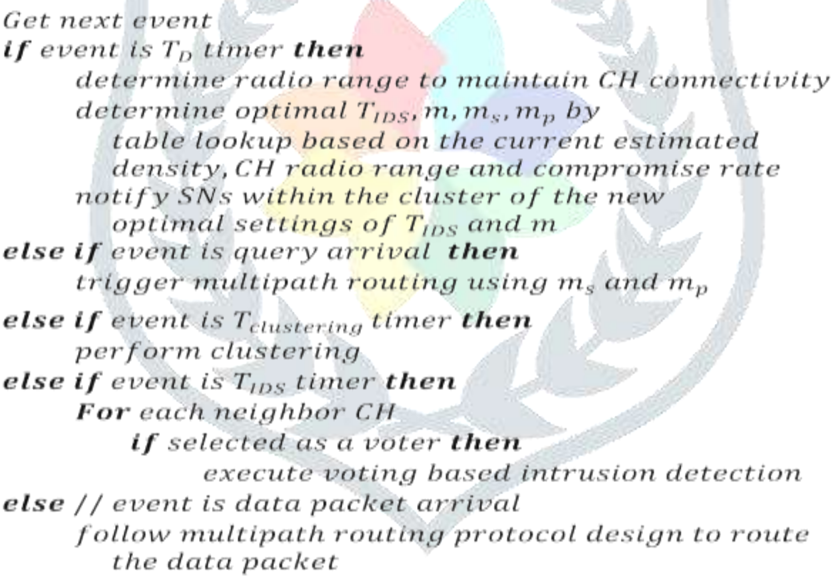
S_{req} is given by:

$$\frac{d_{SN-CH}+d_{CH-PC}}{\text{Treq}}$$

we can estimate the average numbers of hops to forward data from a SN to the source CH, denoted by N^{h}_{SC} and the average numbers of hops to forward data from the source CH to the For redundancy management we create m_p paths between source ch and PC and Path redundancy.

5. ALGORITHM FOR DYNAMIC REDUNDANCY

CH Execution:



```
Get next event
if event is $T_D$ timer then
    determine radio range to maintain CH connectivity
    determine optimal $T_{IDS}, m, m_s, m_p$ by
        table lookup based on the current estimated
        density, CH radio range and compromise rate
    notify SNs within the cluster of the new
        optimal settings of $T_{IDS}$ and $m$
else if event is query arrival then
    trigger multipath routing using $m_s$ and $m_p$
else if event is $T_{clustering}$ timer then
    perform clustering
else if event is $T_{IDS}$ timer then
    For each neighbor CH
        if selected as a voter then
            execute voting based intrusion detection
else // event is data packet arrival
    follow multipath routing protocol design to route
        the data packet
```

Fig. 2: CH execution for dynamic redundancy management.

SN Execution:

```
Get next event
if event is $T_D$ timer then
    determine radio range to maintain SN connectivity
      within a cluster
else if event is control packet arrival from CH then
    Change the optimal settings of $T_{IDS}$, and m
else if event is $T_{clustering}$ timer then
    perform clustering
else if event is $T_{IDS}$ timer then
    For each neighbor SN
        if selected as a voter then
            execute votingbased intrusion detection
else if event is data packet arrival then
    follow multipath routing protocol design to route
      the data packet
```

Fig. 3: SN execution for dynamic redundancy management

Our algorithm for dynamic redundancy management of multipath routing is distributed in nature. Figs. 2 and 3 describe the CH and SN execution protocols, respectively, for managing multipath routing for intrusion endurance to maximize the system lifetime. They specify control actions taken by individual SNs and CHs in response to dynamically changing environment All nodes in the system act periodically to a "TD timer" event to adjust the optimal parameter setting in response to changing environments. This is indicated on line 3 in both Fig. 2 for a CH and Fig. 3 for a SN.

This query arrival event and the action taken are specified on lines 7-8 in Fig.2. When a data packet arrival event occurs, each node simply follows the prescribed multipath routing protocol to route the packet (lines 15–16 in Fig. 2 and lines 13–14 in Fig. 3). Finally each node periodically performs clustering as prescribed by the cluster algorithm, i.e., when a $Tclustering$ timer event occurs, each node executes clustering (lines 9–10 in Fig. 2 and lines 7–8 in Fig. 3)

6. PERFORMANCE EVALUATION

Table II lists the set of input parameter values characterizing a clustered HWSN. Our example HWSN consists of 3000 SN nodes and 100 CH nodes, deployed in a square area of A^2 ($200m \times 200m$). Nodes are distributed in the area following a Poisson process with density λSN = 30 nodes/ ($20 \times 20\ m^2$) and λCH = 1 node/($20 \times 20\ m^2$) at deployment time. The radio ranges rSN and rCH are dynamically adjusted between 5m to 25m and 25m to 120m respectively to maintain network connectivity. The energy dissipation Eelec to run the transmitter and receiver circuitry is 50 nJ/bit.

Fig. 4 shows a high level description of the computational procedure to determine the optimal redundancy level (mp, ms) for maximizing MTTF. The accumulation of queries is shown on line 13. The value of Nq is computed on line 32. Lines 7 and 8 contain the conditions.

```
Input: Table II input parameters
Output: $optimal\ MTTF, optimal\ (m_p, m_s)$
    for $m_s \leftarrow 1$ to $maxMs$ do
      for $m_p \leftarrow 1$ to $maxMp$ do
        $num_q \leftarrow 0$      where $num_q$ is the query counter
        $E_{init}^{SN} \leftarrow N_{SN}(t) \times E_0^{SN}, E_{init}^{CH} \leftarrow N_{CH}(t) \times E_0^{CH}$    where $t = 0$
        Compute $\lambda_{SN}, \lambda_{CH}, R_q, E_{clustering}^{SN}, E_{clustering}^{CH}$
                $E_q^{SN}, E_q^{CH}, E_{IDS}^{SN}, E_{IDS}^{CH}$, at $t = 0$
        Compute arrival time for next clustering,
                query, and IDS events at $t = 0$
        while [ $E_{init}^{SN} > E_{threshold}^{SN}$ and $E_{init}^{CH} > E_{threshold}^{CH}$

      $ev \leftarrow next\ event$
      if $ev$ is clustering event then
        $E_{init}^{SN} = E_{init}^{SN} - E_{clustering}^{SN}, E_{init}^{CH} = E_{init}^{CH} - E_{clustering}^{CH}$
      else if $ev$ is query event then
        $num_q \leftarrow num_q + 1$
        $E_{init}^{SN} = E_{init}^{SN} - E_q^{SN}, E_{init}^{CH} = E_{init}^{CH} - E_q^{CH}$
        if $num_q = 1$ then //first quer
          $rq\ muls \leftarrow rq\ muls \times R_q$
          $temp \leftarrow num_q \times rq\ muls$
        else //terminate previous quer
          $tempMttf \leftarrow tempMttf + temp \times (1 - R_q)$
          $rq\ muls \leftarrow rq\ muls \times R_q$
          $temp \leftarrow num_q \times rq\ muls$
      else // e
        Update distribution of good and bad nodes
        Compute $Pfp$ and $Pfn$
          $E_{init}^{SN} = E_{init}^{SN} - E_{IDS}^{SN}, E_{init}^{CH} = E_{init}^{CH} - E_{IDS}^{CH}$
      Remove Bad caught and Good misidentified nodes
        Compute $Q_c^{SN}, Q_c^{CH}$
         Update $\lambda_{SN}, \lambda_{CH}, N_{SN}, N_{CH}, r_{SN}, r_{CH}$
         Update $R_q, E_{clustering}^{SN}, E_{clustering}^{CH}, E_q^{SN}, E_q^{CH}$
         $tempMttf \leftarrow tempMttf + temp$
         $Mttf \leftarrow tempMttf$
         $N_q \leftarrow num_q$
if $Mttf > optimalMttf$ then
  $optimalMttf \leftarrow Mttf$
  $optimal\ (m_p, m_s) \leftarrow (m_p, m_s)$
            $optimalMttf$ and $optimal\ (m_p, m_s)$
```

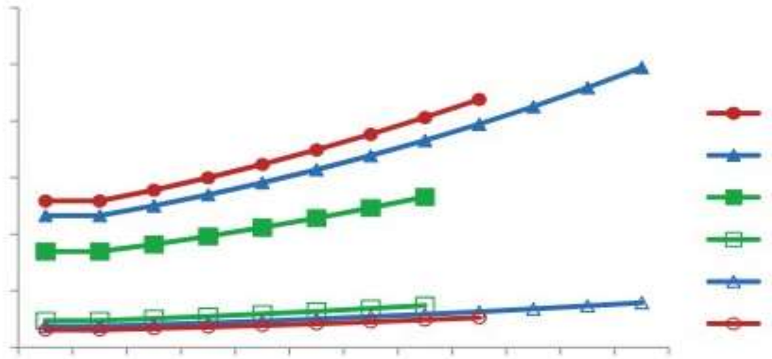


Fig. 4: Computational procedure to determine optimal (m_p, m_s) for maximizing MTTF

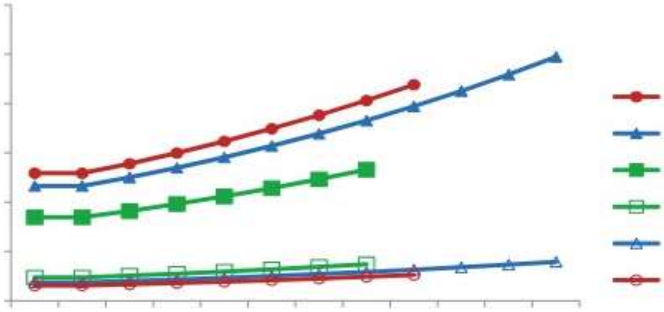


Fig.5: Effect of (m_p, m_s) on energy of CHs and SNs

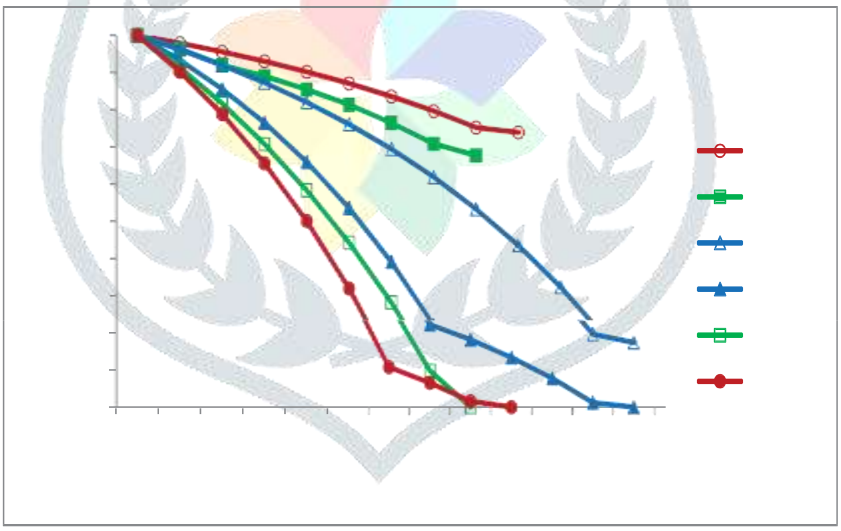


Fig. 6.effect of (mp, ms) on radio range of CHs and SNs

CONCLUSION

In this paper, we performed a tradeoff analysis of energy consumption vs. QoS gain in trustworthiness, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. We developed a novel contingency model to analyze the best redundancy level in terms of path redundancy (*mp*) and source redundancy (*ms*), as well as the best intrusion detection settings in terms of the number of voters (*m*) and the intrusion invocation interval (*TIDS)* under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the trustworthiness, timeliness and security in the presence of unreliable wireless communication and malevolent nodes.

Here we are exploring more extensive malevolent attacks in addition to packet dropping and bad mouthing attacks, each with different implications to energy, security and trustworthiness, and investigate intrusion detection and multipath routing based endurance protocols to react to these attacks.

REFERENCES:

[1] Machado, N. Ansari, G. Wang, and S. Tekinay, “Adaptive density control in heterogeneous wireless sensor networks with and without power management,” *IET Commun.*, vol. 4, no. 7, pp. 758–767, 2010.

[2] E. Stavrou and A. Pitsillides, “A survey on secure multipath routing protocols in WSNs,” *Comput. Netw.*, vol. 54, no. 13, pp. 2215–2238, 2010.

[3] T. Shu, M. Krunz, and S. Liu, “Secure data collection in wireless sensor networks using randomized dispersive routes,” *IEEE Trans. Mobile Comput.*, vol. 9, no. 7, pp. 941–954, 2010.

[4] Y. X. Jiang and B. H. Zhao, “A secure routing protocol with mali- cious nodes detecting and diagnosing mechanism for wireless sensor networks,” in *Proc. 2007 IEEE Asia-Pacific Service Comput. Conf.*, pp. 49–55.

[5] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” in *Proc. 2003 IEEE Int. Workshop Sensor Netw. Protocols Appl.*, pp. 113–127.

[6] B. Deb, S. Bhatnagar, and B. Nath, “ReInForM: reliable information forwarding using multiple paths in sensor networks,” in *Proc. 2003 IEEE Conf. Local Computer Netw.*, pp. 406–415.

[7] G. Bravos and A. G. Kanatas, “Energy consumption and trade-offs on wireless sensor networks,” in *Proc. 2005 IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, pp. 1279–1283.

[8] S. Qun, “Power management in networked sensor radios a network energy model,” in *Proc. 2007 IEEE Sensors Appl. Symp.*, pp. 1–5.

[9] C. Haowen and A. Perrig, “PIKE: peer intermediaries for key estab- lishment in sensor networks,” in *Proc. 2005 IEEE Conf. Computer Commun.*, pp. 524–535.

[10] S. Zhu, S. Setia, and S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks,” in *Proc. 2003 ACM Conf. Computer Commun. Security*.

[11] V. Bhuse and A. Gupta, “Anomaly intrusion detection in wireless sensor networks,” *J. High Speed Netw.*, vol. 15, no. 1, pp. 33–51, 2006.

[12] S. Rajasegarar, C. Leckie, and M. Palaniswami, “Anomaly detection in wireless sensor networks,” *IEEE Wireless Commun. Mag.*, vol. 15, no. 4, pp. 34–40, 2008.

[13] F. Bao, I. R. Chen, M. Chang, and J. Cho, “Hierarchical trust manage- ment for wireless sensor

networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 2, pp. 161–183, 2012.

[14] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," in *Proc. 2003 Conf. IEEE Computer Commun.*, pp. 1713–1723.

[15] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor net- works," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002.

[16] C. J. Fung, Z. Jie, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans. Netw. Service Manage.*, vol. 8, no. 2, pp. 79–91, 2011.

[17] S. Ozdemir, "Secure and reliable data aggregation for wireless sensor networks," in *Proc. 2007 Int. Conf. Ubiquitous Comput. Syst.*

[18] I. R. Chen and T. H. Hsi, "Performance analysis of admission control algorithms based on reward optimization for real-time multimedia servers," *Performance Evaluation*, vol. 33, no. 2, pp. 89–112, 1998.