An Efficient Channel-Aware Detection Mechanism For Wireless Sensor Networks

Akhila Rajeev K, Shinu Acca Mani

Computer Science and Engineering Department

Nehru College of Engineering and Research Centre,Thrissur, India

Abstract - Wireless sensor networks (WSNs) are reliant to selective forwarding attacks that cut back maliciously drop a subset of forwarding packets to decline network performance and jeopardize the information integrity.In this paper, a Channel-aware Reputation System mutually adaptive detection threshold (CRS-A) to identify selective forwarding attacks in WSNs. The CRS-A evaluates the message forwarding behaviours of sensor nodes, according to the abnormality of the monitored packet loss and the estimated normal loss. To optimize the detection truthfulness of CRS-A, theoretically figure the optimal threshold for forwarding analysis, which is adaptive to the time varied channel condition and the estimated attack probabilities of compromised nodes. Furthermore, an attack-tolerant message forwarding schema is created to collaborate with CRS-A for stimulating the forwarding service of compromised nodes and improving the data propagation ratio of the network.Also provide security for forwarding packet by using SHA 256

Keywords: wireless sensor network, selective forwarding attack, reputation system, packet dropping, channel-aware, routing..

I. INTRODUCTION

As a promising event monitoring and data gathering technique, wireless sensor network (WSN) has been widely applied to both military and civilian applications.WSN vulnerable to various security threats. One of the most severe threats is selective forwarding attack, where the compromised nodes can maliciously drop a subset of forwarding packets to deteriorate the data delivery ratio of the network. It also has significantly negative impacts to data integrity.The selective forwarding attacks are concealed by the normal packet losses, complicating the attack detection.

Therefore, it is challenging to detect the selective forwarding attacks and improve the network performance.Since the main challenge of attack detection is to distinguish the malicious drop from normal packet loss, the normal packet loss rate of the transmission link should be considered in the forwarding evaluation. For example, a source node Ns sends 10 packets to the destination node Nd via two forwarding nodes Na and Nb, respectively. Na forwards 6 packets to Nd, while Nb only forwards 5 packets to Nd. Intuitively, Na behaves better than Nb during the data forwarding. However, if the normal packet loss rates from Ns to Na and Nb are 20% and 50%, respectively, Na should have a higher probability to misbehave in this data forwarding. Therefore, consider the deviation between the normal losses and actual losses as the key factor to detect selective forwarding attacks.

(i) Propose CRS-A, which evaluates the forwarding behaviours of sensor nodes by utilizing an adaptive detection threshold. By theoretically analyzing its attitude, make an optimal detection threshold for evaluating the forwarding behaviours to optimize the detection truthfulness of CRS-A. The optimal detection threshold is enthusiastic for each transmission link in a probabilistic manner, and can further be adaptive to the time-varied channel requirement and the attack probability of the forwarding node.

(ii) Develop a distributed and attack-tolerant message forwarding schema to collaborate mutually CRS-A for stimulating the forwarding cooperation of compromised nodes and improving the data propagation ratio of the network. Rather than isolating all the compromised nodes from data forwarding, it jointly considers the time-varied channel requirement and attack probabilities of adjacent nodes in choosing forwarding nodes.

(iii) Extensive simulation results prove that the proposed CRS-A with attack-tolerant data forwarding schema can advance a steep detection accuracy with both of false and missed detection probabilities bring to a close to 0, and improve more than 10% data propagation ratio for the network.

II. SYSTEM MODEL

A. Network Model

Consider a WSN consisting of a set of randomly distributed sensor nodes, denoted by N, and a sink node to monitor an open area. Each sensor node periodically senses the interested information from the surroundings, and transmits the sensed data to the sink via multi-hop routing among sensor nodes. Sensor nodes communicate with their neighboring nodes based on the IEEE 802.11 DCF. The monitored area has an unstable radio environment, making the packet loss rates during the communications of sensor nodes significantly increased and vary from time to time. Since sensor nodes are deployed in open area and lack adequate physical

protection, they may be compromised by adversaries through physical capture or software vulnerabilities to misbehave in data forwarding. Use PM to denote the compromising probability of sensor node, which is defined as the probability that a sensor node is compromised by the adversary. Meanwhile, assume that sensor nodes can monitor the data forwarding traffic of their neighboring nodes by neighbor monitoring with Watchdog or acknowledgment based approaches. It means that a sensor node can obtain that how many data packets are forwarded by its forwarding sensor nodes. Existing works provide a comprehensive study on monitoring forwarding traffic of sensor nodes, which is not the focus of this paper. Since the unstable radio environment causes fluctuated packet loss rates between the neighboring nodes, it is challenging to distinguish the monitored forwarding behaviour is normal or not.

B. Attack Model

Compromised sensor nodes can launch selective forwarding attacks to degrade the performance of the network. Specifically, when a compromised sensor node receives a data packet, it maliciously drops it with a probability, referred to as attack probability. Since the adversary can control the attack probabilities of compromised nodes, it is difficult to distinguish if the packet losses are caused by fluctuated channel condition or malicious drops, especially for the nodes with low attack probabilities.Furthermore, several neighboring compromised sensor nodes can collaborate with each other to launch promotion/demotion attacks to achieve benefits. For example, if Na and Nb are two neighboring compromised sensor nodes and data traffic is from Na to Nb, Na may provide a partial evaluation for Nb's forwarding behaviours. Besides, Na can announce Nb as a normal node to its other neighboring nodes, in spite of Nb misbehaving in the data forwarding.

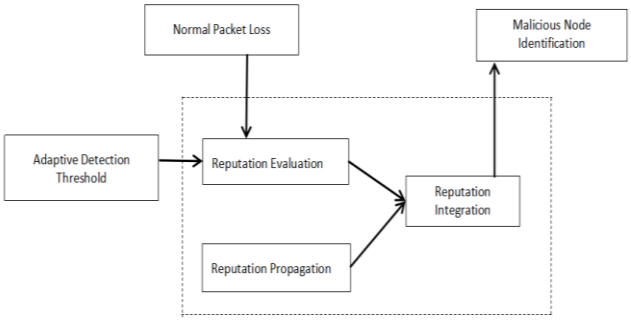

Fig 2.1 System Architecture

However, do not consider the special case where Na is totally honest in data forwarding to cover for Nb's misbehaviours to achieve benefits. This case can be effectively addressed by the hop-byhop acknowledgment or two directional neighbor monitoring techniques. Consider that cryptographic techniques have been utilized in the network to provide sufficient data confidentiality and authentication against the adversary, then focus on resisting selective forwarding attacks. In addition, assume there are only a fraction of sensor nodes compromised by the adversary to misbehave in data forwarding, since the network would be useless if the majority of sensor nodes are manipulated by the adversary. In the following, call the compromised sensor nodes as malicious nodes, and the other sensor nodes as normal nodes.

Modules are mentioned below

In this stipulation, propose CRS-A to identify selective forwarding attacks and detect malicious nodes. In CRS-A, each sensor node maintains a reputation table to consider the long-term forwarding behaviours of its adjacent nodes. The essence of CRS-A is to dynamically create the reputation table based on the forwarding process evaluation for the neighboring nodes, by acquiring the normal packet loss rate into consideration.

1. Reputation Evaluation : In CRS-A, sensor nodes watch their neighbors to evaluate reputation scores for their forwarding behaviours around each evaluation period. The evaluated reputation scores is voiced as first-hand reputation scores. Specifically, in the message transmission stage of T_t, node N_i ($N_i \in N$) records the number of data packets sent to its next hop node N_j as $S_{i,j}(t)$, and the number of data packets forwarded by N_j as $f_{i,j}(t)$. Thus, the number of data packets obliterated in the transmission from N_i to Nj is $m_{i,j}(t) = S_{i,j}(t) - f_{i,j}(t)$. Based on the contention of the previous subsection, estimates the normal packet loss rate surrounded by N_i and N_j as $p_{i,j}(t)$. Since each data packet is transmitted to N_j alone, the data transmission from N_i to N_j can be regarded as a sequences of independent repeated trials. It shows, if N_i sends l data packets to N_j , the probability of k ($0 \le k \le l$) out of l packets obliterated during the transmission, denoted by $P_{i,j}(X = k)$, follows a binomial distribution, i.e.,

$$P_{i,j}(X = k) = \binom{l}{k} (p_{i,j}(t))^k (1 - p_{i,j}(t))^{l-k}.$$

Consider the forwarding fashion evaluation for N_j during an evaluation continuance T_t as a sampling test. If N_j behaves normally around data forwarding, $m_{i,j}(t)$ should slightly fluctuate over the estimated number of normal lost data packets $p_{i,j}(t) \cdot S_{i,j}(t)$.

$$r^1_{i,j}(t) = \begin{cases} +\delta, & \text{if } m_{i,j}(t) \le p_{i,j}(t) \cdot S_{i,j}(t) \\ -\delta, & \text{if } p_{i,j}(t) \cdot S_{i,j}(t) < m_{i,j}(t) \le \xi_{i,j}(t) \\ -\lambda, & \text{if } m_{i,j}(t) > \xi_{i,j}(t) \end{cases}$$

However, when $m_{i,j}(t) > p_{i,j}(t) \cdot S_{i,j}(t)$, with the growth of $m_{i,j}(t)$, the probability of N_j misbehaving in data forwarding increases. In decision to evaluate $m_{i,j}(t)$, plug a

detection threshold $\xi_{i,j}(t)$ ($S_{i,j}(t) \cdot p_{i,j}(t) < \xi_{i,j}(t) < S_{i,j}(t)$, $\xi_{i,j}(t) \in N^+$) and define the reputation evaluation function of N_i to N_j as follows.

where λ is a loss of credit factor and δ is a adjustment factor. Apply $\lambda \gg \delta$ and acknowledge the function as follows.

• If $m_{i,j}(t) \le p_{i,j}(t) \cdot S_{i,j}(t)$, the sampling verify is sufficient, which means the transmission between N_i and N_j is successful. Thus, N_i rewards a doubtless δ to N_j .

• If $p_{i,j}(t) \cdot S_{i,j}(t) < m_{i,j}(t) \le \xi_{i,j}(t)$, we consider it is a normal deviation of $p^m_{i,j}$ around pi,j , and rate $-\delta$ to N_j to neutralize the reputation evaluation.

• When $m_{i,j}(t) > \xi_{i,j}(t)$, approach there is a high probability for N_j to defy in the data forwarding. If it happens, N_i rates a punishment $-\lambda$ to N_j .

2. Reputation Propagation : The monitored forwarding fashion information and hereafter to invigorate the attack detection authenticity, Ni propagates the first-hand reputation scores, such as $r^1_{i,j}(t)$, to their neighbors around each Tt. The received reputation scores from the neighboring nodes are called as secondhand reputation scores, which serves the analysis of the neighboring nodes on their next hop nodes.

Denote the set of N_i's adjacent sensor nodes as NC_i, and the number of nodes in NC_i as $|NC_i|$. Also divide the nodes of NC_i into two subsets, $NC_{i,g}$ and $NC_{i,b}$, based on their long-term reputation values in Ni. Let N_s be a node of NC_i. Take Ns into the honest neighbor set $NC_{i,g}$, if

$$\frac{R_{i,s} > \Sigma_{x \in NCi} R_{i,x}}{|NC_i|}$$

Otherwise, N_s is allocated to the dishonest neighbor set $NC_{i,b}$. Therefore, the second-hand reputation score of N_i to its adjacent node N_j as

$$r^2_{i,j}(t) = \sum_{x \in NC_{i,g}} \frac{R_{i,x}}{\sum_{s \in NC_i} R_{i,s}} \cdot r^1_{x,j}(t) + \sum_{x \in NC_{i,b}} \frac{R_{i,x}}{\sum_{s \in NC_i} R_{i,s}} \cdot \alpha r^1_{x,j}(t)$$

where α is a penalty factor to cut the weight of the information propagated by the potentially dishonest neighbors and $\alpha < 1$.

Since the long-term reputation values of vicious nodes may decrease after misbehaving in a number of evaluation periods, these nodes are categorized into the dishonest neighbor set and the weights of their propagating information are reduced by the penalty factor α. As a result, the negative impacts of reputation promotions among neighboring malicious nodes can be removed

3. Reputation Integration : The first-hand and second-hand short-term reputation scores should be integrated as

$$R^I_{i,j}(t) = \sigma\, r^1_{i,j}(t) + (1 - \sigma) r^2_{i,j}(t).$$

Here, σ is the weight factor of the first-hand information and $\sigma > 0.5$.

4. Malicious Node Identification : In each T_t, sensor nodes can evaluate the forwarding behaviours of their next hop sensor nodes . After a number of evaluation periods, the reputation values of vicious nodes are significantly decrease in the reputation values of their neighboring nodes. To detect the vicious nodes, sensor nodes send their reputation to the sink for detection after a fixed time. When the average reputation value in N_j 's neighbors is below R_a, i.e.,

$$\frac{\sum_{N_i \in NC_j} R_{i,j}}{|NC_j|} < R_a$$

N_j is identified as a malicious node. Here, R_a is an alarm reputation value that can be predefined by system requirements.

5. Attack Tolerant Data Forwarding : To obtain a better forwarding node to surge the data delivery ratio, offer the proposed data forwarding ratio (DFR), which is defined as the ratio between the expected number of forwarded data packets and the total number of sent data packets.In each evaluation continuance T_t, N_i selects the node with the highest DFR from its forwarding candidate set as the next hop. The forwarding candidate set of N_i is the set of its adjacent nodes that are closer to the sink than N_i.

6. Encryption Of Forwarding Packet : Encryption is done by using SHA 256 . it consist of 64 rounds operating on 64 byte blocks where the operations use 64-bit integer arithmetic.

Let M be a message of x bytes, $x = 64n + r$, $0 \le m < 64$

If $r \le 55$, the number of calls to _update() is (n+1)

If $r > 55$, the number of calls to _update() is (n+2)

Denote n = floor (x/64), r = x mod 64, and the cost (in CPU cycles) of one SHA-256 _update() function by UPDATE256. The number of cycles for computing the SHA-256 of M is approximated by

$$\text{UPDATE256} \cdot (n + 1 + \text{floor}(r/55))$$

III. PREVIOUS WORK

This essence of schemes is to regard acknowledgments from diverse nodes in the routing orientation to verify the packet loss rate of each hop and recognize the attackers [1],[2], [3]. Xiao et al. [4] propose a schema that randomly chooses a number of intermediate nodes along a forwarding path as checkpoints to return

acknowledgments for each received packet. If suspicious manner is detected, it generates an alarm packet and delivers it to the source node. Shakshuki et al. [5] design and implement an intrusion-detection program, voiced Enhanced Adaptive Acknowledgement (EAACK), for mobile ad hoc networks. Due to the high load of hop-by-hop acknowledgments, EAACK combines a two-hop acknowledgment schema and an end-to-end acknowledgment schema to notice the vicious behaviours and reduce the network overhead. In addition, EAACK adopts a digital signature with acknowledgment to prove authentication, integrity, and non-repudiation. As an elastic evaluation schema, reputation program is further applied to attack detection. Zhang et al. [6] develop an audit-based misbehaviour detection program to yield reputation administration, trustworthy route exposure, and identification of misbehaving nodes based on behaviour audits in ad hoc networks. In [7], the correlations between link errors and vicious drops are examined to identify selective forwarding attacks. In term to guarantee truthful calculation for the correlations, they propose a Homomorphic Linear Authenticator (HLA) based public auditing construction that allows the detector to prove the authenticity of acknowledgments declared by nodes.

With the Watchdog hardware sensor nodes can inspect the forwarding behaviours of their adjacent nodes and record the certain packet loss accurately. Suat Ozdemir investigates a pragmatic reputation based proper data combination method at variance with selective forwarding attacks in clustered WSNs. Each node maintains a reputation table to evaluate the behaviours of its neighbor nodes, based on the forwarding monitoring of the adjacent nodes. The nodes with reticent reputation values are abandoned from the routing path. However, the reputation analysis is only based on the monitored packet loss around the forwarding. Hao et al. design a repeated game based behave to scan the collusion on selective forwarding attacks in multi-hop wireless networks. Li et al. propose a Side Channel Monitoring (SCM) schema to recognize selective forwarding attacks in wireless ad hoc networks. SCM consider the nodes adjacent to a data communication route, to consist of a side channel for monitoring the forwarding behaviours of the nodes en route. Once misbehaviours are detected, the monitoring nodes send alarm packets to the source node through both channels. Besides these two categories of countermeasures, multi-path routing is further a chiefly applied technique to reduce the impact of selective forwarding attacks on data propagation rather than recognize them . The upshot is to divide each data packet into M shares by a (T,M)-threshold confidential sharing algorithm. Each packet share is assigned a TTL (time to live) function and forwarded by a randomly selected adjoining node. As the TTL decreases afterwards each transmission, the arbitrary forwarding is repeated until TTL decreases to 0. As long as the destination receives T shares, the original message can be effectively reconstructed. In such a behaviour, the data integrity can be guaranteed.

Most of familiar works discussed above can mitigate the negative impacts of selective forwarding attacks on information integrity and network performance. However, they have restrictive capability to accurately recognize the attacks and detect the compromised sensor nodes. In this proposed work, explain an adaptive threshold to evaluate the data forwarding behaviours, which can optimize the detection truthfulness of the reputation system. Moreover, develop an attack-tolerant routing schema collaborating with the reputation program to stimulate the cooperation of compromised nodes for an improved data delivery ratio.

IV. SIMULATION/EXPERIMENTAL RESULTS

In this stipulation, we consider the performance of CRS-A and the attack-tolerant routing schema by the simulations on ns2. The simulation scheme consists of 50 stationary sensor nodes uniformly distributed. Each sensor node has a probability P_M to be compromised as a vicious node, the rate of which is identified in different simulations. The attack probability of each vicious nodes N_j is randomly initialized as a value $p_j \in [0.1, 0.6]$. Each sensor node generates 10 data packets to transmit to the sink via multi-hop routing in each evaluation period.Only suggest no retransmission technique is applied in the simulation, where we can only bring to a focus on the impacts of selective forwarding attacks on data integrity.

CRS-A updates the reputation values of sensor nodes based on their characteristics in data forwarding. The sensor nodes with low reputation values will be identified as vicious nodes

over a number of inspection periods. Compare the reputation values of divergent sensor nodes in 30 evaluation periods. The compromising fortuity is PM = 37% in the simulation. It means that a sensor node has a probability of 37% expected compromised as a vicious node. A larger compromising probability manner a larger number of malicious nodes in the network. As discovered in fig 4.1, the reputation value of the normal sensor node is bit by bit increased after 30 periods, meanwhile the reputation values of malicious node decrease with divergent rates. As conceive as a malicious node increases its attack probability, its reputation rate would suffer a dramatic drop afterwards several inspection periods.

Consider the expected attack-tolerant routing scheme in this subsection, in terms of the data delivery ratio of the network. In term to disclose the improvement definitely,need to compare the attack-tolerant routing schema with the attackavoid routing schema, where sensor nodes indiscriminately isolate the vicious nodes with low

reputation values (below the alarm value Ra) from the routing path. Fig. 4.2 shows the packet delivery ratio comparison of the couple routing scheme over 50 analysis periods. Both of the routing schemes are applied with CRS-A to the network. The compromising probability of sensor nodes is PM = 25%, and the security check is performed at the 45-th period, which can update all the identified vicious nodes to be normal. As shown in the figure, the sooner significant improvement of the data delivery ratio is in the inspection periods [0, 15] for both routing schemes, where the vicious nodes with steep attack probabilities are detected and desolate from the routing path. Meanwhile, after the security examine, both routing schemes experience an improvement on data delivery ratio due to the removal of vicious nodes. However, in the periods from 20 to 44, the attack-tolerant routing scheme has a greater than 10% improvement on data delivery ratio, compared with the attack-avoid routing scheme. That is because the vicious nodes with good channel condition and low attack probabilities are selected into the routing path, and stimulated to perform better to avoid a reputation punishment.

The security of data should be assured using SHA 256. So it provide greater authenticity,integrity. SHA-2 is a cryptographic hash function, and is a building block for various cryptographic constructs. In satisfying the requirements of cryptographic hash, it's a one-way function that is deterministic, expeditious to compute, resistant to pre-image and second-preimage attacks, and is collision resistant. scrypt is a password-based key derivation function. It's used to turn a low-entropy password into a cryptographic key or verifier with effectively higher entropy by being intentionally slow to compute. It's tunable to drive larger amounts of CPU and/or memory as technology advances, making hardware dedicated to computing it all expensive.

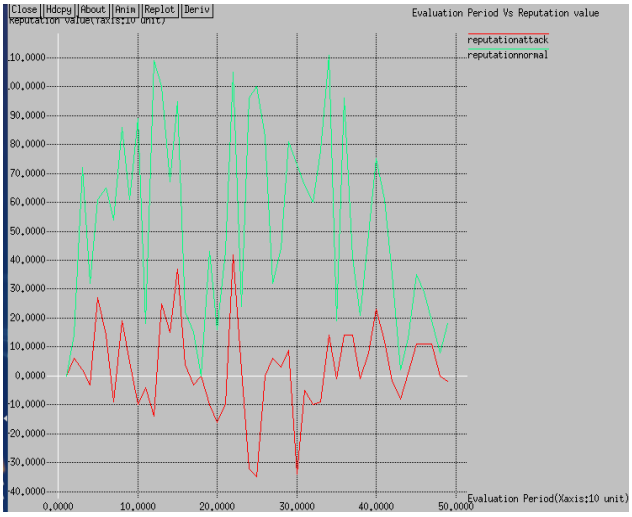

Fig. 4.1. Reputation value comparison.

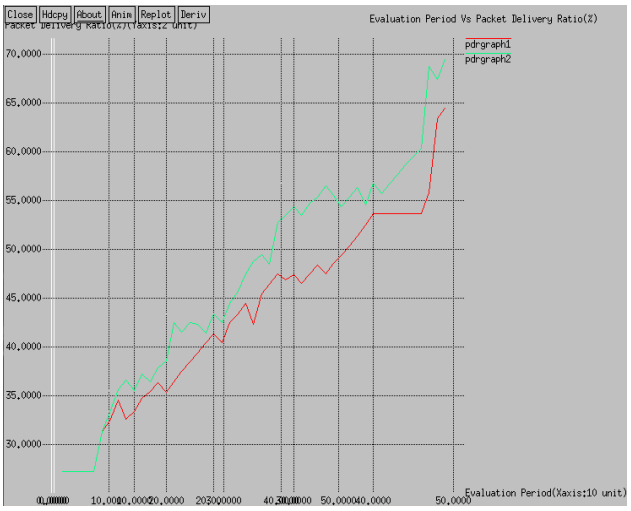

Fig. 4.2. Packet delivery ratio comparison

V. CONCLUSION

Proposed a channel-aware reputation system by all of adaptive detection threshold (CRS-A) to recognize selective forwarding attacks in WSNs. To successfully distinguish selective forwarding attacks from the normal packet loss, CRSA evaluates the forwarding behaviours by the abnormality between the estimated normal packet loss and monitored packet loss. To invigorate the detection truthfulness of CRS-A, further derived the optimal analysis threshold of CRS-A in a probabilistic approach, which is adaptive to the time varied channel condition and the attack probabilities of compromised nodes. In basic principle, a distributed and attack-tolerant data forwarding schema is created to collaborate by the whole of CRS-A for stimulating the use of compromised nodes and improving the data propagation ratio.Also provide security for forwarding packet by using SHA 256.Simulation results disclose that the proposed CRS-A can progress a steep detection truthfulness with low false and missed detection probabilities, and the proposed attack tolerant data forwarding schema can recover more than 10% data visit from the stork scale for the network.

REFERENCES

[1] Ju Ren, Yaoxue Zhang, Kuan Zhang, and Xuemin (Sherman)Shen, “Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks” IEEE Transactions On Wireless Communications, Vol. XX, No. XX, XXX 2016

[2] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, “An acknowledgment based approach for the detection of routing misbehaviour in manets,” IEEE Trans. Mob. Comput., vol. 6, no. 5, pp. 536–550, 2007.

[3] E. Mahmoud and X. Shen, “An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks,” IEEE Trans. Vehic. Tech., vol. 60, no. 8, pp. 3947–3962, 2011.

[4] B. Xiao, B. Yu, and C. Gao, "Chemas: Identify suspect nodes in selective forwarding attacks," J. Parallel Distributed Comput., vol. 67, no. 11, pp. 1218–1230, 2007.

[5] H.-Y. Lin and W.-G. Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

[6] E. Shakshuki, N. Kang, and T. Sheltami, "Eaacka secure intrusiondetection system for manets," IEEE Trans. Ind. Electro., vol. 60, no. 3,pp. 1089–1098, 2013.

[7] Y. Zhang, L. Lazos, and W. Kozma, "Amd: Audit-based misbehaviour detection in wireless ad hoc networks," IEEE Trans. Mob. Comput., prePrints, published online in Sept. 2013.

[8] T. Shu and M. Krunz, "Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing," in Proc. ACM WiSec, 2012, pp. 87–98.