International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 02, Issue – 12, December – 2017, PP – 73-81

Advanced Audit-based Misbehaviour Detection in Networks

Shivani Nikam, Shweta Joshi, Vaishali Sakhare, Divya Jagtap,
Prof. Jitendra Musale

Abstract: We address the problem of identifying and isolating misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks, we develop a system called Advance Audit-based Misbehavior Detection in network that effectively and efficiently isolates both continuous and selective packet droppers.
Advance Audit-based Misbehavior Detection in network System integrates reputation management, trustworthy route discovery and identification of misbehaving node based on behavioral audits.
Advance Audit-based Misbehavior Detection in network detects selective dropping attacks even if end-to-end traffic is encrypted and can be applied to multi channel networks or networks consisting nodes, even when large portion of network refuses to forward packets.
Index Terms: Misbehaviour, Packet dropping, Reputation System, Recovery.

INTRODUCTION

In the absence of a supporting infrastructure, wireless ad hoc networks realize end To end communications in a cooperative manner. Nodes rely on the establishment of multi hop routes to overcome the limitations of their finite communication range. Moreover, selfish nodes may mis-configure their devices to refuse forwarding traffic in order to conserve energy. This type of behavior is known as node misbehavior. Existing solutions for identifying misbehaving nodes either use some form of per-packet evaluation of peer behavior. On the other hand, per packet behavior evaluation techniques are based on either transmission overhearing or achieving of per packet acknowledgement. This type of monitoring operations must be repeated on every hop of a multihop route, thus it require high communication Overhead and energy expenditure. Also, they fail to detect dropping attacks of selective nature, since intermediate monitoring nodes may not be aware of the desired selective dropping pattern to be detected. Reputation based systems use neighboring monitoring techniques to evaluate the behavior of nodes and reputation values are given to node according to its functionality of packet forwarding Objectives are Provide an effective mechanism to deal with misbehaving nodes in the network.

- Effectively and efficiently detection of both continuous selective packet dropping
- Encourage co-operation among nodes in the network
- Minimize computation overhead at each node
- Detection of misbehaving link and node in parallel

Wireless Sensor Networks (WSNs) can be used in a broad range of applications from complex military operations to simple domestic environments. This makes security a vital characteristic in WSNs. There have been numerous studies in the field of security

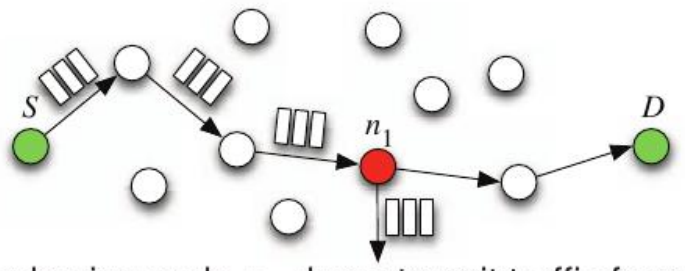
AMD is a comprehensive solution that integrates identification of misbehaving nodes, reputation management, and trustworthy route discovery in a distributed and resource- efficient manner. We develop the AMD system for detecting and isolating misbehaving nodes. Compared to state-of-the-art

AMD provides the following additional features:

1) AMD enables the per-packet evaluation of a nodes behavior without incurring a per-packet overhead .
2) AMD enables the concurrent first-hand evaluation of the behavior of several nodes that are not necessarily one- hop neighbors. Overhearing techniques are limited to one hop.
3) AMD can operate in multi-channel networks and in networks with directional antennas. Current packet overhearing techniques are only applicable when transmissions can be overhead by peers operating on the same frequency band.
4) AMD detects selective dropping behaviors by allowing the source to perform matching against any desired selective dropping patterns. This is particularly important when end to- end traffic is encrypted. In the latter scenario, only the source and destination have access to the contents of the packets and can detect selective dropping.

We show that AMD can construct paths consisting of highly trusted nodes, subject to a desired path length constraint. When paths contain misbehaving nodes, these nodes are efficiently located by a behavioral audit process. We map the problem of identifying misbehaving nodes to the classic R`enyi-Ulam game of 20 questions. The identification strategy is supplemented by the knowledge of nodes reputation.

Packet dropping:



Misbehaving node n_1 drops transit traffic from S to D.

In a wireless ad hoc network, nodes communicate with each other via wireless links either directly or relying on other nodes as routers. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network. An adversary may misbehave by agreeing to forward packets and then failing to do so. Once being included in a route, the adversary starts dropping packets. That means it stop forwarding the packet to the next node. The malicious node can exploit its knowledge about the protocol to perform an insider attack. It can analyze the importance of the transmitting packet and can selectively drop those packets. Thus it can completely control the performance of the network. If the attacker continuously dropping packets, it can be detect and mitigate easily. Because even if the malicious node is unknown. If the malicious nodes getidentified, the node can be deleted from the routing table of network. The detection of selective packet dropping is highly difficult. Sometimes the dropping of packets may not be intentional. It can be occurred as a result of channel errors. So the detection mechanism should be capable of differentiating the malicious packet dropping and the dropping due to link errors. The algorithm introduced here provides an efficient mechanism to detect the selective packet dropping.

Attacker:

Attacker is one who makes changes the energy of particular nodes in router. And all attackers details stored in router with their all details such as attacker Ip address, attacked node, modified energy and attacked time. The use cases in the proposed system include browse file, initialize node, send file, select node, inject less energy, capture attack detection, view all traffic patterns, select less distance node, find traffic nodes, find drop packets, resend dropped packets, view attackers, receive file, save file and request dropped packets.

A. Existing System :

In existing System misbehaving nodes either use some form of pre-packet evaluation of peer behavior or provide corporate incentives to stimulate participation. In this system transmission overhearing or issuance of per-packet behavior evaluation techniques and leading to high communication overload and energy expenditure. They fail to detect dropping attacks of selective nature sine intermediate monitoring nodes may not be aware desired selective dropping pattern to be detected.

Disadvantages:

1) Energy expenditure is high.
2) Traffic related issues.
3) Low performance of network.

B. Proposed System

We develop a system called AMD: Audit Based Misbehavior detection in Wireless Ad Hoc Network Which helps to pre-packet behavior detection (AMD) without incurring a per-packet per-hop cost? is a comprehensive solution that integrates identification of misbehaving nodes, reputation management and trusty route discovery in distributed and resource efficient manner.

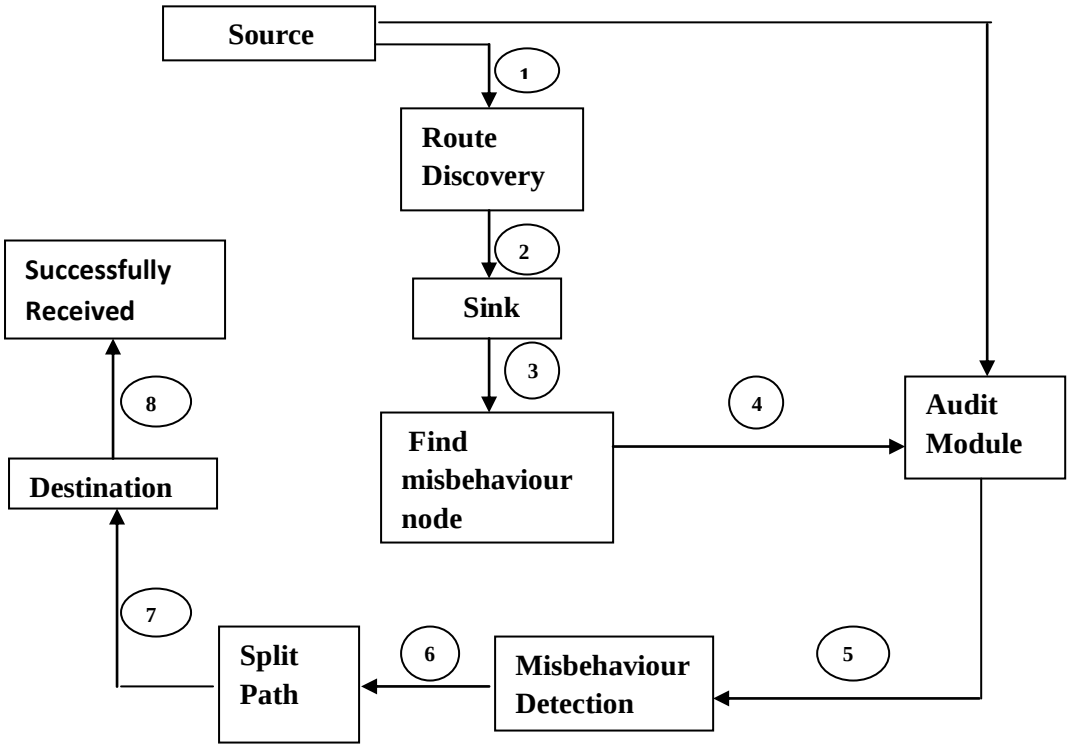


Fig. System Architecture Flow

Advantages:
1) Small amount energy expenditure for packet transmission.
2) Increase network performance.
3) Reduce the time for transmission.
4) Maintain audit record of failure packet.

AMD provides a comprehensive misbehavior identification and node isolation system for eliminating misbehavior from a given network. This system consists of the integration of three modules: a *reputation* module, a *route discovery* module, and an *audit* mod-ule. These modules closely interact to coordinate the functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers. A schematic of the relationship between the three modules of AMD.

The reputation module is responsible for managing reputation information based on the recommendations of the audit module. Reputation values are exploited by the route discovery module for establishing routes that exclude nodes with low reputations.

Finally, the audit module efficiently identifies misbehaving nodes via an audit process. This process is accelerated based on input received from the reputation module. We note that while several techniques have been proposed for reputation management and reputation-based route discovery, in AMD, we develop novel methods for these two functions that integrate efficiently with the per-flow behaviour evaluation implemented by the audit module. We now describe the three modules in detail.

Modules:

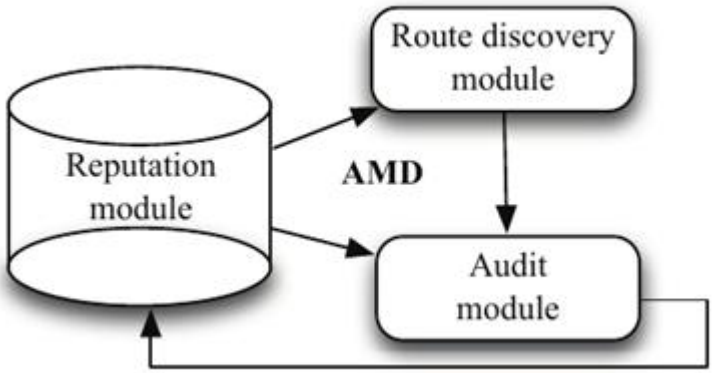


Fig.System Module

1) Reputation Module.
2) Route discovery Module.
3) Audit Module.

1) Reputation Module:

The reputation module is responsible for computing and managing the reputation of nodes.

We adopt a decentralized approach in which each node maintains its own view of the reputation of other nodes. Such implementation alleviates the communication overhead for transmitting information to a centralized location, and readily translates to the distributed nature of ad hoc networks.

We take into account both first-hand and second-hand information. Information is considered to be first-hand if it is obtained by direct interaction between nodes (e.g., node ni routes information via node nj), and is considered to be second-hand if it is indirectly obtained based on the opinions of other nodes [22]. Consideration of both first-hand and second hand information has been shown to improve the reliability of reputation metrics [13], [21], [22].

First-hand information: A reputation evaluation is considered to be first-hand, if it originates from the audit module running on ni. This is because the audit module can make direct observations of the behavior of nodes in a path PSD based on behavioral audits.

we have adopted the AIMD(additive increase/multiplicative decrease) principle in order to rapidly isolate a misbehaving node from routing paths. Due to the multiplicative factor (α), the reputation of a misbehaving node rapidly declines with repeated misbehavior. On the other hand, a node with a low reputation would require significant time (in epochs) until its reputation is restored, due to the additive increase factor (β).

Second-hand information: Second-hand information is used only if first-hand information becomes stale, or is not available due to the lack of prior interaction between two nodes.

If no 2^{nd} hand information available, the reputation value restored to last known 1^{st} hand information, Also 1^{st} hand information becomes available it replace the second hand information.Audit module running on on source makes evaluations on behaviour of each node along the path. This evaluation are considered as 1^{st} hand information for source.

In 1^{st} module we computes only reputation value source for PSD.

2) Route discovery Module:

The route discovery module is responsible for the discovery of trustworthy paths from a source to a destination. Whenever there is no cached path to the destination then source invoked route discovery module. To step the trustworthiness of a path, we define the following path reputation.

Path reputation value: The reputation of a path defined by product of reputation value of all node of particular path. If in this path, any node (malcious) haing low reputation value due to this low reputation values of path decreases.

Discovery of Trustworthy Routes:

To discover trustworthy routes, we modify the discovery phase of the DSR(Dynamic Source Routing) protocol. In DSR, when S(source) has packets for D(destination), it checks whether a route exists in its cache. If a route does not exist, S broadcasts a Route Request (RREQ) message. This message contains the source ID, destination ID, and the time to-live (TTL)1. Any intermediate node that receives the RREQ, appends its ID to the RREQ message and rebroadcasts it while decreasing the TTL field by one unit. If a receiving node is the destination, D responds to S with a route reply (RREP) message containing the entire PSD. The RREP follows the reverse path to S.

The basic operation of source S to destination D through the intermediate nodes of B and C are performed and it is shown below:

MESSAGE PROCESS

Route request (RREQ) process:

Initiator node

o Initiate a RREQ to target o Intermediate nodes

- previously seen RREQ→ take no action o Else
- If not target→ append id to path and retransmit RREQ
- If target→ take actions below in RREP

Route reply RREP process:

Target node

o Calculate and attach signature over the path in the received RREQ

o Unicast the RREP

Intermediate nodes (along the unicast path)

o If not initiator

- Calculate and attach signature over the received RREP
- Transmit updated RREP to next upstream` host

o If initiator

- Validate the accumulated path against the target signature
- Validate individual signatures to ensure that every node in target signature has supplied a signature in the reverse path order

BASIC OPERATION:

S → *: (RREQ, S, D, id, ()) B → *: (RREQ, S, D, id, (B))
C → *: (RREQ, S, D, id, (B, C))
D → C: (RREP, S, D, (B, C), (sigD))
C → B: (RREP, S, D, (B, C), (sigD, sigC))
B → S: (RREP, S, D, (B, C), (sigD, sigC, sigB)

3) Audit Module:

The audit module is responsible for identifying the set of nodes that misbehave in a particular path PSD. The source invokes the audit module if it detects poor performance on PSD. The exact definition of what constitutes poor performance can be determined on the basis of a specific application running between S and D.

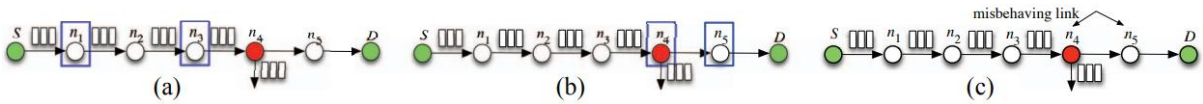
When poor performance is detected over PSD, the source requests from a subset of intermediate nodes to record a digest of the set of packets they forward to the next hop. We call this, the audit process. Although misbehaving nodes can lie when audited, audit replies from honest nodes lead to the identification of those lies, and eventually of the misbehaving nodes. We map the audit process to Renyi-Ulam searching games [25], [29].

Algorithms:

1) Reputation-based Audit Algorithm (CUT):

Initialize: $\mathcal{V} = \{n_l, \ldots, n_r\}$, $n_l \leftarrow n_1, n_r \leftarrow n_k$
while $|\mathcal{V}| > 2$
{ $h \leftarrow \arg\min_{\mathcal{V}} r_S^i$
audit(n_{h-1})
if $a_{h-1} = 0$
$n_r \leftarrow n_{h-1}$
else
{ audit(n_{h+1})
if $a_{h+1} = 1$
$n_l \leftarrow n_{h+1}$
else
{ audit(n_h)
if $a_h = 0$
$n_r \leftarrow n_h$
else
$n_l \leftarrow n_h$ }}}
audit(n_l, n_r)
if $a_l \neq a_r$
return n_l, n_r
else
return $|M| \geq 2, Partition\ P_{SD}$

Define the set of nodes suspicious of misbehavior as V.
n is audited node
r is reputation value
k is last malicious node.
h is honest.
a is misbehaving link
misbehaving nodes |M| on a single path.



(a) Let V1 = {n1,...,n5} with A = {n1, n2, n3}, B = {n4, n5} and nω = n4. The source audits A, concluding nω ∈/ A.
(b) The source then audits B, concluding nω ∈ B.
(c) The source proceeds to stage 2 with V2 = {n4, n5}. Since |V2| = 2, link {n4, n5} is identified to be the misbehaving one.

2] Membership Questioning Algorithm (MEM)

$\mathcal{V}_1 = \{n_l, \ldots, n_r\}, n_l \leftarrow S, n_r \leftarrow D, \Phi = \emptyset$
while $|\mathcal{V}_j| > 2$
$\{ \quad h = \lceil \frac{|\mathcal{V}_j|}{2} \rceil, \quad \phi_{1,a} = audit(n_i, n_h)$
if $a_i \neq a_j|$
$\Phi \leftarrow \{\phi_{j,a}\}$
$j = j + 1, \quad \mathcal{V}_j = \{n_l, \ldots, n_h\}$
else
$\{ \quad \phi_{j,b} = audit(n_h, n_k)$
if $a_h \neq a_r$
$\Phi \leftarrow \{\phi_{j,a}, \phi_{j,b}\}$
$j = j + 1, \quad \mathcal{V}_j = \{n_h, \ldots, n_r\}$
else
return $j = j - 1$, new_partition$(\mathcal{V}_{j-1})\}\}\}$
return n_l, n_r

V1 = {n1,...,nk}. Set V1 is divided into two subsets, A = {n1,...,ni} and B = {ni+1,...,nk} with i = |V1| 2 . The source first asks "Is nω ∈ A?" by simultaneously auditing nodes n1, ni. If n1 and ni return conflicting audit claims, i.e., a1 = 1, ai = 0, the source knows that nω ∈ A, adds φ1,a to Φ, and proceeds to stage two with V2 = {n1,...,ni}. If a1 = ai = 1, the source questions "Is nω ∈ B?" by simultaneously auditing nodes ni, nk. If ni, nk return ai = ak, the source concludes that nω ∈ B, adds {φ1,a, φ1,b} to Φ, and proceeds with V2 = {ni,...,nk}. If ai = ak, the source concludes a lie has occurred, returns to the previous stage, and chooses another partition for V1.

Performance Evolution:

We randomly deployed 100 nodes within an area of 100m×100m. A fraction of these nodes was randomly selected to misbehave. The misbehaving nodes independently implemented a packet dropping strategy, either continuous or selective. The reputation of each node was initialized to 0.5. We randomly selected 1,000 source/destination pairs from the set of honest nodes. For each pair, we ran the route discovery module to construct a trustworthy path. In each session, the source routed 10,000 packets to the destination via the established path. To isolate the performance degradation due to malicious dropping, lower layer details such as contention and retransmissions due to collisions were abstracted. In our simulations, packet dropping due to channel conditions was implemented as a dropping module on each node, similar to that of misbehavior. Each experiment was repeated for 50 random network topologies. All our simulations were performed using a stand-alone Java-based simulator that implemented the AMD module at every node of the network.

Sender:

Node Sender selects the file which is to present. And then it split into the number of packets based on the size for adding some bits in it. And then it encrypts all the splitted packets. Sender adds some bits to each encrypted packets before sending that. Bit Addition for each packet is identification for sender. After adding of bits to each packet, it sends the packets to the nearest node or intermediate node. The intermediate node receives Packets from the sender. After receiving all packets from sender, it encrypts all packets again for authentication[1]. Before sending to sink, intermediate add some bits to each packet for node identification. After adding some bits from intermediate, it sends all packets to the sink. Before sending all packets to sink, packets dropping or packets modifying may be occur in intermediate.

Sink:

Sink receives all packets from the sender node, and it verifies all packets which are dropped or not. And it also verifies the packets which are modified or not and it can identify the modifiers in the process based on the bit identification. After receiving all packets in sink, it decrypts all packets. After the decryption if there is no modified or dropped packets, it merge all packets. After merging, Sink can receive the original file.

Conclusion:

We developed AMD, a comprehensive misbehavior detection and mitigation system which integrates three critical functions: reputation management, route discovery, and identication of misbehaving nodes via behavioral audits. We modeled the process of identifying misbehaving nodes as Renyi-Ulam games and derived resource efficient identication strategies. We showed that AMD recovers the network operation even if a large fraction of nodes is misbehaving at a signicantly lower communication cost. Moreover AMD can detect selective dropping attacks over end to end encrypted traffic streams.

Future Scope:

In proposed system, AMD detect the misbehaving node in the large network also recovers the network operation even if a large fraction of node is misbehaving at a significant lower communication cost. In Future, we used this system for various campaigning for example, if we want to sell large no of product to the end user, through the clients. So in this example, we used AMD system for detection of misbehaviour of client at the time of unsuccessful delivery.

References:

[1]. Data Exchange in Ad-Hoc Network Using AMD Two- step Authentication Framework International Journal of Emerging Research in Management Technology
1) Pournima Sadhu,
2) R.C.Roychaudhary

[2]. Secure Routing And Attack Detection In Wirelesss Adhoc Network International Journal On Engineering Technology and Sciences
1) Dr.C.Kumar Charliepaul
2) K.Megala Devi

[3]. A Survey and analysis of reliable data packet delivery ratio in wireless Sensor Network SSRG Inter-national Journal of Mobile Computing Application
1)Subramanan.P.
2)Soundarya.M

[4]. Privacy And Detecting Malicious Dropping In Wireless Ad -Hoc Network Journal Of Engineer- ing And Computer Science
1) M. Sindhuja
2) Mrs A.Sahaya Princy M.Tech

[5]. Detection of routing misbehavior in MANET using im- proved 2ACK IOSR Journal of Computer Engineering
1) Prof. Poonam Gupta
2) Sarita Chopde

[6]. A Survey on Adaptive and Channel Aware Detection of Selective Forwarding Attacks in Ad-Hoc Networks Inter- national Journal of Innovative Research in Computer and Communication Engineering
1) Samira Sayyed
2) Madhuri Waghule Rupali Patil

[7]. A Survey on Reputation System And Price System Based Cooperation Inducement Scheme In Mobile Adhoc Networks International Journal of Engineering Trends and Technology
1) Manikandan.
2) Muthukumarasamy.
3) Thanigaivelu.

[8]. K. Hansen, T. Larsen, and K. Olsen. On the efciency of fast rsa variants in modern mobile phones. Arxiv preprint arXiv:1001.2249, 2010.Packet Dropping In Wireless Ad -Hoc Network Journal Of Engineer- ing And Computer Science
1)M. Sindhuja
2) Mrs A.Sahaya Princy M.Tech

[9]. S. Soltanali, S. Pirahesh, S. Niksefat, and M. Sabaei. An Efficient Scheme to Motivate Cooperation in Mobile Ad hoc Networks. In Proc. of ICNS, Pages 92–98, 2007.

[10]. D. Stinson. Cryptography: theory and practice. CRC press, 2006.

[11]. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens.ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information System Security, 10(4):11–35, 2008

[12]. G. Acs, L. Buttyan, and L. Dora. Misbehaving router detection in link-state routing for wireless mesh networks. In Proc. of WoWMoM, pages 1–6, 2010.

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

[14]. Detection of routing misbehavior in MANET using im- proved 2ACK IOSR Journal of Computer Engineering
1) Prof. Poonam Gupta
2) Sarita Chopde

[15]. A Survey on Adaptive and Channel Aware Detection of Selective Forwarding Attacks in Ad-Hoc Networks Inter- national Journal of Innovative Research in Computer and Communication Engineering
1) Samira Sayyed
2) Madhuri Waghule Rupali Patil

[16]. A Survey on Reputation System And Price System Based Cooperation Inducement Scheme In Mobile Adhoc Networks International Journal of Engineering Trends and Technology
1) Manikandan.
2) Muthukumarasamy.
3) Thanigaivelu.

[17]. K. Hansen, T. Larsen, and K. Olsen. On the efciency of fast rsa variants in modern mobile phones. Arxiv preprint arXiv:1001.2249, 2010.

